IMPLEMENTIERUNGSLEITFADEN

EMC VSPEX-ANWENDER-COMPUTING

VMware Horizon View 6.0 und VMware vSphere für bis zu 500 virtuelle Desktops

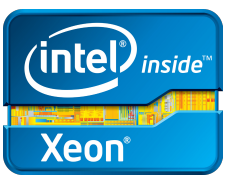
Unterstützt durch EMC VNXe3200 und EMC Datensicherheit

EMC VSPEX

Zusammenfassung

Dieser Implementierungsleitfaden beschreibt die allgemeinen Schritte für die Bereitstellung einer EMC® VSPEX®-Lösung für Anwender-Computing für VMware Horizon View und VMware vSphere, unterstützt durch das EMC VNXe3200™-Speicherarray und EMC Datensicherheit.

Oktober 2014



EMC²

Copyright © 2014 EMC Deutschland GmbH. Alle Rechte vorbehalten. Veröffentlicht in Deutschland

Veröffentlicht im Oktober 2014

EMC ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Die Informationen in dieser Veröffentlichung werden ohne Gewähr zur Verfügung gestellt. Die EMC Corporation macht keine Zusicherungen und übernimmt keine Haftung jedweder Art im Hinblick auf die in diesem Dokument enthaltenen Informationen und schließt insbesondere jedwede implizite Haftung für die Handelsüblichkeit und die Eignung für einen bestimmten Zweck aus. Für die Nutzung, das Kopieren und die Verteilung der in dieser Veröffentlichung beschriebenen EMC Software ist eine entsprechende Softwarelizenz erforderlich.

EMC², EMC und das EMC Logo sind eingetragene Marken oder Marken der EMC Corporation in den USA und anderen Ländern. Alle anderen in diesem Dokument erwähnten Marken sind das Eigentum ihrer jeweiligen Inhaber.

Eine aktuelle Liste der Produkte von EMC finden Sie unter EMC Corporation Trademarks auf germany.emc.com.

EMC VSPEX-Anwender-Computing
VMware Horizon View 6.0 und VMware vSphere für bis zu 500 virtuelle Desktops
Unterstützt von EMC VNXe3200 und EMC Datensicherheit
Implementierungsleitfaden

Art.-Nr.: H12935.1

Inhalt

Kapitel 1 Einleitung 7
Zweck dieses Leitfadens ... 8
Geschäftlicher Nutzen ... 8
Umfang ... 9
Zielgruppe ... 9
Terminologie ... 10

Kapitel 2 Bevor Sie beginnen 11
Überblick ... 12
Aufgaben vor der Bereitstellung ... 12
Bereitstellungsworkflow ... 13
Grundlegende Dokumente ... 14
VSPEX-Lösungsüberblick ... 14
VSPEX-Designleitfaden ... 14
VSPEX Proven Infrastructure-Leitfaden ... 14
EMC Datensicherheit für VSPEX ... 14
Leitfaden zu RSA SecurID für VSPEX-Anwender-Computing ... 14
Voraussetzungen für die Bereitstellung ... 14

Kapitel 3 Lösungsüberblick 17
Überblick ... 18
Bewährte VSPEX-Infrastruktur ... 18
Lösungsarchitektur ... 19
High-Level-Architektur ... 19
Logische Architektur ... 21
Übersicht über die wichtigen Komponenten ... 22

Kapitel 4 Lösungsimplementierung 23
Überblick ... 24
Vorbereiten der Netzwerkinfrastruktur ... 25
Konfigurieren der Netzwerkinfrastruktur ... 25
Konfigurieren der VLANs ... 26
Konfigurieren des Speichernetzwerks (Blockvariante) ... 26
Vervollständigen der Netzwerkverkabelung ... 27
Vorbereiten und Konfigurieren des Speicherarrays ... 27
Vorbereiten der VNXe ... 29
Einrichten der anfänglichen VNXe-Konfiguration ... 29
Provisioning von Kerndatenspeicher ... 29
Provisioning von Speicher für VMFS-Datastores (nur Block) ... 29

Provisioning von Speicher für NFS-Datastores (nur Datei) 31
Konfigurieren von FAST Cache 33
Provisioning von optionalem Speicher für Benutzerdaten 35
Provisioning von optionalem Speicher für virtuelle Infrastrukturmaschinen 35
Festlegen der Schwellenwerte und Warnmeldungen für Virtual Provisioning 36
Installation und Konfiguration der VMware vSphere-Hosts 36
Installieren von vSphere 37
Konfigurieren des vSphere-Netzwerks 37
Verbinden der VMware-Datastores 38
Installation und Konfiguration der SQL Server-Datenbank 38
Bereitstellen von VMware vCenter Server 40
Einrichten von VMware Horizon View Connection Server 41
Erstellen virtueller Maschinen für die VMware Horizon View Connection Server 43
Installieren von VMware Horizon View Connection Server 43
Konfigurieren der Verbindung zur View-Ereignisprotokolldatenbank 43
Hinzufügen einer View Connection Server-Replikatinstanz 43
Konfigurieren der View Composer-ODBC-Verbindung 43
Installieren von View Composer 43
Verbinden von VMware Horizon View mit vCenter und View Composer 43
Vorbereiten einer virtuellen Master-Maschine 44
Konfigurieren von View Persona Management-Gruppen-Policies 44
Konfigurieren von Gruppen-Policies für die Ordnerumleitung für EMC Avamar 44
Konfigurieren von View PCoIP-Gruppen-Policies 45
Provisioning von virtuellen Desktops 45
Einrichten von EMC Avamar 46
Einrichten von VMware vShield Endpoint 47
Überprüfen der Desktop-Treiberinstallation für vShield Endpoint 48
Bereitstellen der vShield Manager-Appliance 48
Anwenden von vShield Endpoint-Lizenzen 48
Installieren des vShield Endpoint-Services 48
Bereitstellen eines Managementservers für die Virenschutzlösung 48
Bereitstellen der virtuellen vSphere-Sicherheitsmaschinen 48
Überprüfen der vShield Endpoint-Funktion 49
Einrichten von VMware Horizon Workspace 49
Zuweisen von IP-Adressen und Erstellen von DNS-Datensätzen 52
Gewähren der SMTP-Relayberechtigungen für Workspace 52
Konfigurieren einer PostgreSQL- oder Oracle-Datenbank für Workspace 52
Konfigurieren einer CIFS-Freigabe zur Verwendung als ThinApp-Repository (optional) 52
Verifizieren der angegebenen E-Mail-Adressen aller Workspace-Benutzer 53
Bereitstellen der Workspace-Appliance für vCenter 53

Erlangen der Informationen, die erforderlich sind, um die Workspace-Integration mit Active Directory zu aktivieren 53
Verwenden eines vertrauenswürdigen SSL-Zertifikats und eines privaten Schlüssels für die Workspace-Appliance (optional) 53
Konfigurieren des externen Zugriffs auf die Workspace-Appliance (optional) 54
Aktivieren der Horizon View-Integration (optional) 54
Einrichten von VMware vCenter Operations Manager for Horizon View 54

Kapitel 5 Lösungsverifizierung 57

Überblick 58
Checkliste nach der Installation 59
Bereitstellen und Testen eines einzigen virtuellen Desktops 59
Überprüfen der Redundanz der Lösungskomponenten 59

Kapitel 6 Referenzdokumentation 61

EMC Dokumentation 62
Andere Dokumentation 62

Anhang A Konfigurationsarbeitsblatt 65

Arbeitsblatt für die Kundenkonfiguration 66

Abbildungen

Abbildung 1. VSPEX Proven Infrastructure 19
Abbildung 2. Architektur der validierten Lösung 20
Abbildung 3. Logische Architektur für Block- und File-Speicher 21
Abbildung 4. Beispiel-Ethernetnetzwerkarchitektur 26
Abbildung 5. Beispiel für eine Fibre-Channel-Netzwerkarchitektur 27
Abbildung 6. Assistent für Speicherpools: FAST Cache 30
Abbildung 7. Konfigurieren der NAS-Serveradresse über das entsprechende Dialogfeld 32
Abbildung 8. FAST Cache-Assistent: Ergebnisbildschirm 34
Abbildung 9. Registerkarte „Advanced“ im Dialogfeld „Storage Pool Properties“ 35
Abbildung 10. Definieren der Schwellenwerte für die Speicherpoolauslastung 36
Abbildung 11. Snapshot-Einstellungen für Speicherpools 36
Abbildung 12. View Composer Disks – Fenster 46
Abbildung 13. Öffnen von Anhängen in einer PDF-Datei 66

Tabellen

Tabella 1. Terminologie 10
Tabella 2. Aufgaben vor der Bereitstellung 12
Tabella 3. Bereitstellungsworkflow 13
Tabella 4. Checkliste für die Bereitstellungsvoraussetzungen 14
Tabella 5. Lösungskomponenten 22
Tabella 6. Überblick über den Implementierungsprozess 24
Tabella 7. Aufgaben für die Switch- und Netzwerkkonfiguration 25
Tabella 8. Aufgaben für die Speicherkonfiguration 28
Tabella 9. Aufgaben für die Serverinstallation 37
Tabella 10. Aufgaben für die SQL Server-Datenbankkonfiguration 39
Tabella 11. Aufgaben für die vCenter-Konfiguration 40
Tabella 12. Aufgaben für die Einrichtung der VMware Horizon View-Verbindungsserver 41
Tabella 13. Für die Installation und Konfiguration von vShield Endpoint erforderliche Aufgaben 47
Tabella 14. Aufgaben für die Einrichtung von VMware Horizon Workspace 49
Tabella 15. Für die Installation und Konfiguration von vCenter Operations Manager erforderliche Aufgaben 54
Tabella 16. Aufgaben für das Testen der Installation 58
Tabella 17. Allgemeine Serverinformationen 66
Tabella 18. vSphere-Serverinformationen 67
Tabella 19. Array-Informationen 67
Tabella 20. Informationen zur Netzwerkinfrastruktur 67
Tabella 21. VLAN-Informationen 67
Tabella 22. Servicekonten 68

Kapitel 1 Einleitung

In diesem Kapitel werden folgende Themen behandelt:

Zweck dieses Leitfadens **8**

Geschäftlicher Nutzen **8**

Umfang **9**

Zielgruppe **9**

Terminologie **10**

Zweck dieses Leitfadens

Mit der EMC® VSPEX®-Architektur für das Anwender-Computing erhält der Kunde ein modernes System, mit dem eine große Zahl virtueller Desktops auf einem konsistenten Performancelevel gehostet werden kann. Diese VSPEX-Anwender-Computing-Lösung für VMware Horizon View 6.0 wird auf einer VMware vSphere-Virtualisierungsebene ausgeführt, die vom EMC VNXe3200™-Array mit hoher Verfügbarkeit unterstützt wird, das den Speicher bereitstellt. Die Lösung wurde für die Ausführung auf einer VSPEX Private Cloud für VMware vSphere Proven Infrastructure entworfen.

Die von den VSPEX-Partnern definierten Rechner- und Netzwerkkomponenten sind redundant und ausreichend leistungsstark ausgelegt, um die Verarbeitungs- und Datenanforderungen einer großen virtuellen Maschinenumgebung zu erfüllen. EMC Avamar®-Datensicherheits- und Recovery-Lösungen bieten Datensicherheit für VMware Horizon View-Daten und RSA® SecurID® stellt eine optionale Funktion für die sichere Benutzerauthentifizierung bereit.

Diese VSPEX-Anwender-Computing-Lösung ist für bis zu 500 virtuelle Desktops validiert. Die validierten Konfigurationen basieren auf einem Referenzdesktop-Workload und bilden die Basis für die Erstellung kostengünstiger, angepasster Lösungen für einzelne Kunden. Eine größere Umgebung mit 2.000 virtuellen Desktops basiert auf der EMC VNX5600™ und ist im *EMC VSPEX-Anwender-Computing: VMware Horizon View 6.0 und VMware vSphere für bis zu 2.000 virtuelle Desktops – Designleitfaden beschrieben.*

Eine Architektur für Anwender-Computing ist ein komplexes Systemangebot. In diesem Implementierungsleitfaden wird beschrieben, wie Sie mithilfe von Best Practices die erforderlichen Ressourcen implementieren, um eine Anwender-Computing-Lösung mit VMware Horizon View für VMware vSphere bereitzustellen, die von EMC VNX3200 und von Lösungen mit EMC Datensicherheit unterstützt wird.

Geschäftlicher Nutzen

Geschäftliche Anwendungen werden zunehmend in konsolidierte Datenverarbeitungs-, Netzwerk- und Speicherumgebungen verlagert. Diese VSPEX-Anwender-Computing-Lösung mit VMware reduziert die Komplexität bei der Konfiguration der einzelnen Komponenten eines herkömmlichen Bereitstellungsmodells. Dabei wird die Komplexität des Integrationsmanagements reduziert, während die Optionen für das Anwendungsdesign und die Implementierung erhalten bleiben. Obwohl die Lösung eine einheitliche Administration bietet, kann die Trennung von Prozessen angemessen kontrolliert und überwacht werden.

Die VSPEX-Anwender-Computing-Lösung für VMware Horizon View bietet unter anderem die folgenden geschäftlichen Vorteile:

- End-to-End-Virtualisierungslösung zur Nutzung der Funktionen von einheitlichen Infrastrukturkomponenten
- Effiziente Virtualisierung von bis zu 500 virtuellen Desktops für verschiedene Kundenanwendungsbeispiele
- Zuverlässige, flexible und skalierbare Referenzarchitekturen

Umfang

In diesem Implementierungsleitfaden werden die allgemeinen Schritte beschrieben, die für die Bereitstellung der VSPEX-Anwender-Computing-Lösung für VMware Horizon View 6.0 erforderlich sind, die auf einer VSPEX Private Cloud für VMware vSphere Proven Infrastructure ausgeführt wird. Sie finden Beispiele für Bereitstellungen auf dem EMC VNXe3200-Speicherarray. Dieselben Prinzipien und Richtlinien gelten auch für alle VNXe®-Modelle, die im Rahmen des VSPEX-Programms validiert wurden.

Lösungen von EMC Datensicherheit für VMware Horizon View sind in einem separaten Dokument beschrieben: *EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View – Design- und Implementierungsleitfaden*.

Die optionale RSA SecurID-Lösung für die sichere Benutzerauthentifizierung für VMware Horizon View wird ebenfalls in einem separaten Dokument beschrieben: *Sicherung des EMC VSPEX-Anwender-Computings mit RSA SecurID: VMware Horizon View 5.2 und VMware vSphere 5.1 für bis zu 2.000 virtuelle Desktops – Designleitfaden*.

Zielgruppe

Dieser Leitfaden richtet sich an interne Mitarbeiter von EMC und qualifizierte EMC VSPEX-Partner. In diesem Leitfaden wird davon ausgegangen, dass VSPEX-Partner, die beabsichtigen, diese VSPEX Proven Infrastructure für VMware Horizon View bereitzustellen, über die erforderliche Schulung und den entsprechenden Hintergrund verfügen, um eine Anwender-Computing-Lösung auf der Basis von Horizon View mit VMware vSphere als Hypervisor, Speichersysteme der VNXe-Serie und die damit verbundene Infrastruktur installieren und konfigurieren zu können.

Leser sollten außerdem mit den Infrastruktur- und Datenbanksicherheitsrichtlinien der Kundeninstallation vertraut sein.

In diesem Leitfaden werden gegebenenfalls externe Referenzen bereitgestellt. Partner, die diese Lösung implementieren, sollten mit diesen Dokumenten vertraut sein. Ausführliche Informationen finden Sie unter Grundlegende Dokumente auf Seite 14 und Kapitel 6, Referenzdokumentation auf Seite 61.

Terminologie

In Tabella 1 führt die in diesem Handbuch verwendete Terminologie auf.

Tabella 1. Terminologie

Begriff	Definition
Anwender-Computing	Das Anwender-Computing entkoppelt den Desktop von der physischen Maschine. In einer Anwender-Computing-Umgebung befinden sich das Desktopbetriebssystem und die Anwendungen auf einer virtuellen Maschine, die auf einem Hostcomputer ausgeführt wird. Die Daten befinden sich auf einem gemeinsamen Speicher. Die Benutzer greifen von einem beliebigen Computer oder Mobilgerät über ein privates Netzwerk oder eine Internetverbindung auf ihren virtuellen Desktop zu.
Verknüpfte Clones	Als verknüpfte Clones bereitgestellte Desktops verwenden ein gemeinsames Basis-Image innerhalb eines Desktoppools und haben deshalb einen minimalen Platzbedarf.
Referenzarchitektur	Eine validierte Architektur, die diese VSPEX-Anwender-Computing-Lösung für bis zu 500 virtuelle Desktops unterstützt
Speicherprozessor (SP)	Der Speicherprozessor (SP) ist die Rechnerkomponente des Speicherarrays. SPs werden für alle Aspekte der Datenverlagerung in, aus und zwischen Arrays eingesetzt.

Kapitel 2 Bevor Sie beginnen

In diesem Kapitel werden folgende Themen behandelt:

Überblick 12

Aufgaben vor der Bereitstellung 12

Bereitstellungsworkflow 13

Grundlegende Dokumente 14

Voraussetzungen für die Bereitstellung 14

Überblick

In diesem Kapitel erhalten Sie einen Überblick über wichtige Informationen, die Sie kennen, Dokumente, mit denen Sie vertraut sein, und Aufgaben, die Sie ausführen müssen, bevor Sie mit der Implementierung der VSPEX-Anwender-Computing-Lösung mit VMware Horizon View beginnen.

Im Designleitfaden für diese Lösung – *EMC VSPEX-Anwender-Computing: VMware Horizon View 6.0 und VMware vSphere für bis zu 500 virtuelle Desktops* – wird beschrieben, wie Sie Ihre Lösung entwerfen und dimensionieren, Ressourcen gemäß Best Practices zuweisen und alle Vorteile nutzen, die VSPEX zu bieten hat. Die Beispiele für Bereitstellungen in diesem Implementierungsleitfaden beruhen auf den Empfehlungen und Beispielen des Designleitfadens.

Aufgaben vor der Bereitstellung

Zu den Aufgaben vor der Bereitstellung zählen Verfahren, die nicht direkt mit der Installation und Konfiguration der Umgebung zusammenhängen, deren Ergebnisse aber zum Zeitpunkt der Installation benötigt werden. Zu den Aufgaben vor der Bereitstellung gehören das Erfassen von Hostnamen, IP-Adressen, VLAN-IDs, Lizenzschlüsseln, Installationsmedien und so weiter. Führen Sie vor einem Besuch beim Kunden die in Tabella 2 beschriebenen Aufgaben durch, um die vor Ort erforderliche Zeit zu verkürzen.

Tabella 2. Aufgaben vor der Bereitstellung

Aufgabe	Beschreibung	Referenz
Sammeln von Dokumenten	Besorgen Sie sich die in Grundlegende Dokumente und Kapitel 6, Referenzdokumentation aufgeführten Dokumente. Auf diese wird in diesem gesamten Dokument Bezug genommen, um Details zu Einrichtungsverfahren und Dimensionierung sowie Best Practices für die Bereitstellung der verschiedenen Komponenten der Lösung zur Verfügung zu stellen.	• Grundlegende Dokumente auf Seite 14 • Referenzdokumentation auf Seite 61
Sammeln von Tools	Sammeln Sie die erforderlichen und optionalen Tools für die Bereitstellung. Prüfen Sie mithilfe von Tabella 4, Checkliste für die Bereitstellungsvoraussetzungen, ob die gesamte Hardware und Software sowie die entsprechenden Lizenzen vor dem Bereitstellungsprozess verfügbar sind.	• Checkliste für die Bereitstellungsvoraussetzungen auf Seite 14

Aufgabe	Beschreibung	Referenz
Erfassen von Daten	Erfassen Sie die kundenspezifischen Konfigurationsdaten für Netzwerk, Arrays, Konten usw. Geben Sie diese Informationen in das Arbeitsblatt für die Kundenkonfiguration ein, das Sie während des Bereitstellungsprozesses als Referenz verwenden können. Füllen Sie zusätzlich für die umfassendsten arrayspezifischen Informationen das *Konfigurationsarbeitsblatt für die VNXe-Serie* aus.	• Arbeitsblatt für die Kundenkonfiguration auf Seite 66 • *Konfigurationsarbeitsblatt für die VNXe-Serie* auf der EMC Online Support-Website

Bereitstellungsworkflow

Ziehen Sie für das Design und die Implementierung Ihrer Lösung den Prozessablauf in Tabelle 3[1] zurate.

Tabelle 3. Bereitstellungsworkflow

Step	aktion
1	Verwenden Sie das Arbeitsblatt für die Kundenkonfiguration im Designleitfaden, um Kundenanforderungen zu erfassen.
2	Verwenden Sie das EMC VSPEX-Dimensionierungstool, um die empfohlene VSPEX-Referenzarchitektur für Ihre Anwender-Computing-Lösung auf der Basis der in Schritt 1 erfassten Benutzeranforderungen zu ermitteln. Weitere Informationen zum Dimensionierungstool finden Sie im EMC VSPEX Sizing Tool Portal. **Hinweis:** Sollte das Dimensionierungstool nicht zur Verfügung stehen, können Sie die Anwendung anhand der Richtlinien im Designleitfaden manuell dimensionieren.
3	Legen Sie das endgültige Design der VSPEX-Lösung mithilfe des Designleitfadens fest. **Hinweis:** Sorgen Sie dafür, dass alle Ressourcenanforderungen und nicht nur die Anforderungen für das Anwender-Computing berücksichtigt werden.
4	Wählen Sie die geeignete VSPEX-Referenzarchitektur und Proven Infrastructure aus und bestellen Sie sie. Empfehlungen zur Auswahl einer Proven Infrastructure finden Sie im folgenden VSPEX Proven Infrastructure-Leitfaden: *EMC VSPEX Private Cloud: VMware vSphere 5.5 für bis zu 125 virtuelle Maschinen*.
5	Befolgen Sie diesen Implementierungsleitfaden zum Bereitstellen und Testen Ihrer VSPEX-Lösung. **Hinweis**: Wenn Sie bereits über eine VSPEX Proven Infrastructure-Umgebung verfügen, können Sie die bereits abgeschlossenen Schritte für die Implementierung überspringen.

[1] Wenn Ihre Lösung Komponenten zur Datensicherung enthält, finden Sie Informationen zur Dimensionierung von Backup und Recovery sowie Implementierungsrichtlinien im *EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View – Design- und Implementierungsleitfaden*.

Grundlegende Dokumente

EMC empfiehlt, dass Sie die folgenden Dokumente lesen, die Sie im Bereich „VSPEX“ im EMC Community Network oder auf den Seiten zur VSPEX Proven Infrastructure unter germany.emc.com finden. Falls Sie auf ein Dokument nicht zugreifen können, wenden Sie sich an Ihren EMC Vertriebsmitarbeiter.

VSPEX-Lösungsüberblick

Lesen Sie das folgende Dokument zur VSPEX-Lösungsübersicht:

- *EMC VSPEX-Lösungen für Anwender-Computing mit VMware vSphere und VMware Horizon View*

VSPEX-Designleitfaden

Lesen Sie die folgenden VSPEX-Designleitfäden:

- *EMC VSPEX-Anwender-Computing: VMware Horizon View 6.0 und VMware vSphere für bis zu 500 virtuelle Desktops*

VSPEX Proven Infrastructure-Leitfaden

Lesen Sie folgenden VSPEX Proven Infrastructure-Leitfaden:

- *EMC VSPEX Private Cloud: VMware vSphere 5.5 für bis zu 125 virtuelle Maschinen*

EMC Datensicherheit für VSPEX

Lesen Sie den folgenden Leitfaden zu EMC Datensicherheit für VSPEX:

- *EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View – Design- und Implementierungsleitfaden*

Leitfaden zu RSA SecurID für VSPEX-Anwender-Computing

Lesen Sie den folgenden Leitfaden zu RSA SecurID:

- *Sicherung des EMC VSPEX-Anwender-Computings mit RSA SecurID: VMware Horizon View 5.2 und VMware vSphere 5.1 für bis zu 2.000 virtuelle Desktops – Designleitfaden*

Voraussetzungen für die Bereitstellung

In Tabella 4 gibt die Hardware-, Software- und Lizenzanforderungen für die Konfiguration der Lösung an. Weitere Informationen zu diesen Voraussetzungen finden Sie auf der EMC Online Support-Website.

Tabella 4. Checkliste für die Bereitstellungsvoraussetzungen

Anforderung	Beschreibung
Hardware	• Physische Server mit ausreichend Kapazität zum Hosten der virtuellen Desktops gemäß den Empfehlungen im Designleitfaden • VMware vSphere-Server zum Hosten der virtuellen Infrastrukturserver • Für das Anwender-Computing erforderliche Netzwerk-Switch-Portkapazität und -funktionen • EMC VNXe-Multiprotokollspeicher-Array mit dem erforderlichen Laufwerkslayout **Hinweis**: Diese Anforderungen werden möglicherweise durch die vorhandene Infrastruktur erfüllt.

Anforderung	Beschreibung
Software	• Installationsmedien für VMware vSphere 5.5 • Installationsmedien für VMware vCenter Server 5.5 • VMware vShield Manager Open Virtualization Appliance (OVA)-Datei • VMware vCenter Operations Manager OVA-Datei • VMware vCenter Operations Manager for Horizon View-Adapter • Installationsmedien für VMware Horizon View 6.0 • Management-Serversoftware für die VMware vShield Endpoint-Virenschutzlösung von Partnern • VMware vShield Endpoint-Partnersoftware für die Sicherheit von virtuellen Maschinen • EMC Virtual Storage Integrator (VSI) für VMware vSphere Web Client OVA-Datei • Installationsmedien für Microsoft Windows Server 2012 R2 (empfohlenes Betriebssystem für VMware vCenter und VMware Horizon View Connection Server) • Installationsmedien für Microsoft Windows 8.1 • Installationsmedien für Microsoft SQL Server 2012 **Hinweis**: Diese Anforderung wird möglicherweise durch die vorhandene Infrastruktur erfüllt.
Software (nur Blockvariante)	• EMC PowerPath® Viewer • EMC PowerPath Virtual Edition (PowerPath/VE)
Lizenzen	• Lizenzschlüssel für VMware vCenter 5.5 • Lizenzschlüssel für VMware vSphere Desktop • Lizenzschlüssel für VMware Horizon View 6.0 • Lizenzschlüssel für VMware vShield Endpoint (VMware) • Lizenzschlüssel für VMware vShield Endpoint (vShield-Partner) • VMware vCenter Operations Manager für VMware Horizon View • Lizenzschlüssel für Microsoft Windows Server 2012 R2 Standard Edition (oder höher) **Hinweis**: Diese Anforderung wird möglicherweise durch einen vorhandenen Microsoft Key Management Server (KMS) erfüllt. • Lizenzschlüssel für Microsoft Windows 8.1 **Hinweis**: Diese Anforderung wird möglicherweise durch einen vorhandenen Microsoft KMS erfüllt. • Lizenzschlüssel für Microsoft SQL Server **Hinweis**: Diese Anforderung wird möglicherweise durch eine vorhandene Lizenz erfüllt.
Lizenzen (nur Blockvariante)	• Lizenzdateien für EMC PowerPath Virtual Edition

Kapitel 3 Lösungsüberblick

In diesem Kapitel werden folgende Themen behandelt:

Überblick **18**

Bewährte VSPEX-Infrastruktur **18**

Lösungsarchitektur **19**

Übersicht über die wichtigen Komponenten **22**

Überblick

In diesem Kapitel finden Sie einen Überblick über die VSPEX-Lösung für Anwender-Computing für VMware Horizon View auf VMware vSphere und die wichtigsten in der Lösung verwendeten Technologien. Die Lösung wurde von EMC entwickelt und erprobt und bietet die für den Support von Referenzarchitekturen mit 500 virtuellen Desktops erforderlichen Ressourcen für Desktopvirtualisierung, Server, Netzwerk, Speicher und Datensicherheit.

Obwohl die Lösung für die Ausführung auf einer VSPEX Private Cloud-Lösung entworfen wurde, enthalten die Referenzarchitekturen keine Konfigurationsdetails für die zugrunde liegende Proven Infrastructure. Informationen zum Konfigurieren der erforderlichen Infrastrukturkomponenten finden Sie im folgenden VSPEX Proven Infrastructure-Leitfaden: *EMC VSPEX Private Cloud: VMware vSphere 5.5 für bis zu 125 virtuelle Maschinen*.

Bewährte VSPEX-Infrastruktur

EMC hat gemeinsam mit den branchenführenden Anbietern von IT-Infrastrukturen eine vollständige Virtualisierungslösung entwickelt, die die Bereitstellung der Private Cloud und der virtuellen VMware Horizon View-Desktops beschleunigt. Mit VSPEX sind Kunden in der Lage, die Umgestaltung ihrer IT durch schnellere Bereitstellung, verbesserte Anwenderfreundlichkeit, größere Auswahl, höhere Effizienz und weniger Risiko zu beschleunigen. Dadurch wird die Erstellung der IT-Infrastruktur vereinfacht.

Die VSPEX-Validierung durch EMC ermöglicht eine zuverlässige Performance und gestattet Kunden die Auswahl von Technologie, die ihre vorhandene oder neu erworbene IT-Infrastruktur nutzt und so den Planungs-, Dimensionierungs- und Konfigurationsaufwand vermeidet. VSPEX stellt eine virtuelle Infrastruktur für Kunden bereit, die die charakteristische Einfachheit von echten konvergenten Infrastrukturen und gleichzeitig mehr Auswahlmöglichkeiten bei den einzelnen Lösungskomponenten erreichen möchten.

Eine VSPEX Proven Infrastructure ist, wie in Abbildung 1 gezeigt, eine modulare, virtualisierte Infrastruktur, die von EMC validiert und von EMC VSPEX-Partnern geliefert wird. Sie umfasst die Virtualisierungs-, Server-, Netzwerk-, Speicher- und Datensicherheitsebene. Partner können die Virtualisierungs-, Server- und Netzwerktechnologien auswählen, die am besten zur Umgebung eines Kunden passen. Gleichzeitig stellen die Speichersysteme der hochverfügbaren EMC VNXe-Serie und Technologien von EMC Datensicherheit die Speicher- und Datensicherheitsebene zur Verfügung.

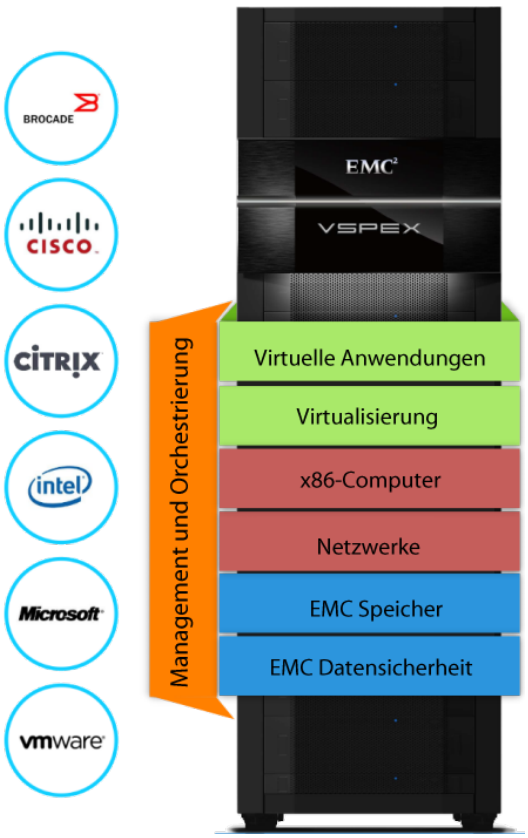


Abbildung 1. VSPEX Proven Infrastructure

Lösungsarchitektur

High-Level-Architektur

Die VSPEX-Lösung für Anwender-Computing für VMware Horizon View bietet eine vollständige, validierte Systemarchitektur, die bis zu 500 virtuelle Desktops unterstützen kann. Die Lösung unterstützt sowohl Block- als auch File-Speicher.

Abbildung 2 zeigt die übergeordnete Architektur der validierten Lösung.

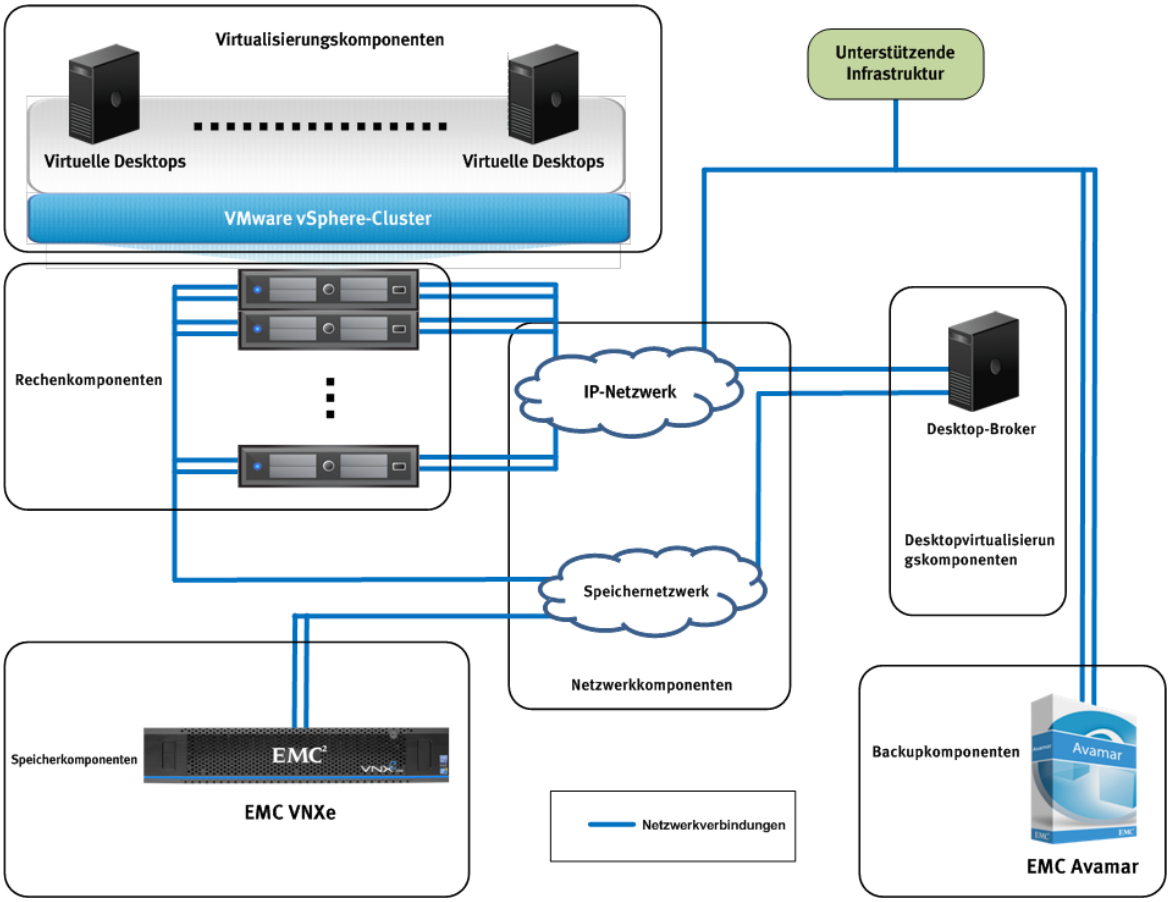


Abbildung 2. Architektur der validierten Lösung

In dieser Lösung werden EMC VNXe und VMware vSphere für die Bereitstellung der Speicher- beziehungsweise Virtualisierungsplattformen für eine VMware Horizon View-Umgebung mit virtuellen, von VMware Horizon View Composer bereitgestellten Microsoft Windows 8.1-Desktops verwendet.

Für diese Lösung haben wir[2] das VNXe3200-Array bereitgestellt, um bis zu 500 virtuelle Desktops zu unterstützen.

Die Lösung ist für die Ausführung auf einer VSPEX Private Cloud für VMware vSphere entworfen und wird von der hochverfügbaren EMC VNXe-Serie unterstützt, die den Speicher bereitstellt. Die Infrastrukturservices für die Lösung, die in Abbildung 3 auf Seite 21 gezeigt sind, können von vorhandener Infrastruktur am Kundenstandort, von der VSPEX Private Cloud oder durch die Bereitstellung der Services als dedizierte Ressourcen im Rahmen der Lösung bereitgestellt werden.

Die Planung und das Design der Speicherinfrastruktur für eine Horizon View-Umgebung ist wichtig, da der gemeinsame Speicher große Belastungsspitzen bei I/O-Vorgängen abfangen können muss, die im Laufe eines Arbeitstags auftreten. Diese Belastungsspitzen können zu Phasen mit einer unregelmäßigen und unzuverlässigen Performance der virtuellen Desktops führen. Benutzer mögen sich an eine langsame Performance gewöhnen, aber eine unzuverlässige Performance führt zu Frustration und verringert die Effizienz.

[2] In diesem Leitfaden bezieht sich „wir“ auf das EMC Solutions Engineering-Team, das die Lösung validierte.

Für eine zuverlässige Performance in Anwender-Computing-Lösungen muss das Speichersystem die Spitzen-I/O-Last der Clients bei minimaler Antwortzeit verarbeiten können. Da die Implementierung vieler Laufwerke zur Verarbeitung kurzer Zeiträume mit extremem I/O-Druck kostspielig ist, wird in dieser Lösung EMC FAST™ Cache verwendet, um die Anzahl der erforderlichen Laufwerke zu reduzieren.

EMC Datensicherheitslösungen ermöglichen den Schutz und die Wiederherstellbarkeit von Anwenderdaten. Dafür werden in dieser Horizon View-Lösung EMC Avamar und der damit verbundene Desktopclient verwendet.

Logische Architektur

Die EMC VSPEX-Lösung für Anwender-Computing für VMware Horizon View enthält 2 Speichertypvarianten: Block und File. Abbildung 3 zeigt die logische Architektur für beide Varianten.

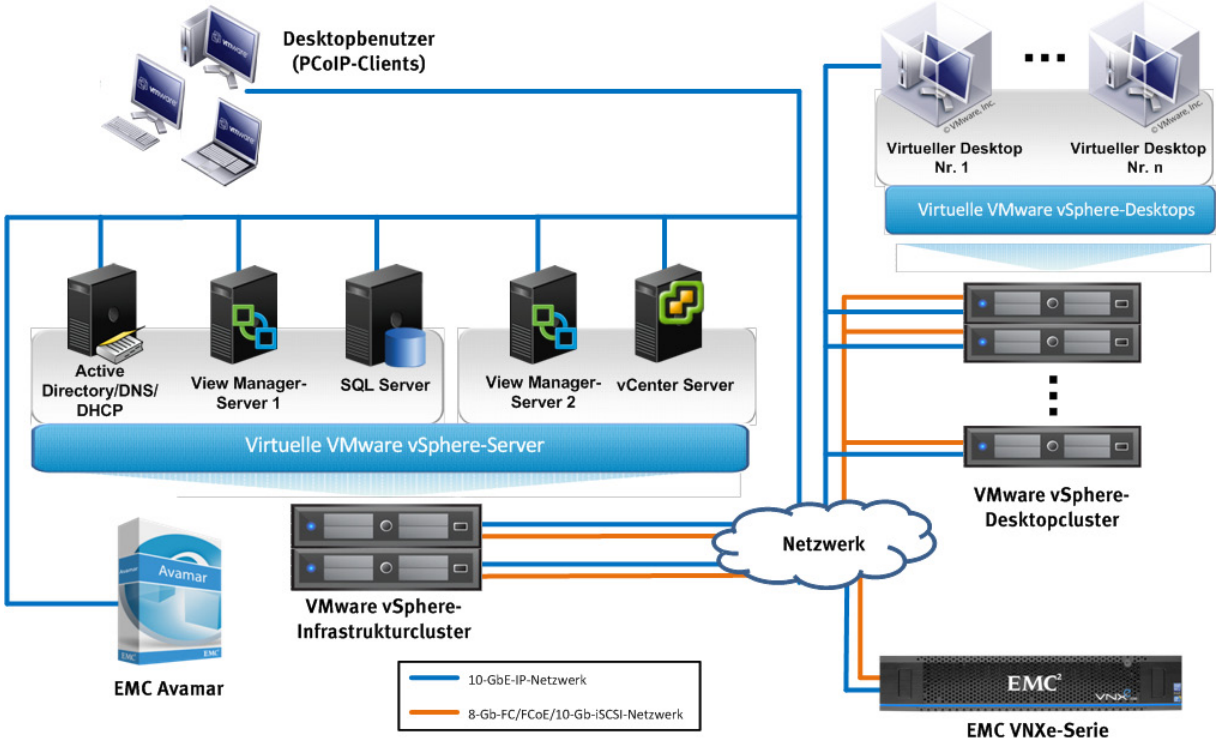


Abbildung 3. Logische Architektur für Block- und File-Speicher

Die Blockvariante verwendet 2 Netzwerke: ein Speichernetzwerk zur Bereitstellung von virtuellen Desktops und virtuellen Serverbetriebssystemdaten sowie ein 10-Gbit-Ethernetnetzwerk (GbE) für den übrigen Datenverkehr. Für das Speichernetzwerk wird 8-Gbit-Fibre-Channel (FC) oder 10 GbE mit iSCSI-Protokoll verwendet. Bei der File-Variante wird ein 10 GbE-IP-Netzwerk für den gesamten Datenverkehr verwendet.

Hinweis: Die Lösung unterstützt darüber hinaus 1 GbE, falls die Bandbreitenanforderungen erfüllt werden.

Übersicht über die wichtigen Komponenten

In Tabella 5 fasst die in dieser Lösung verwendeten wichtigen Technologien zusammen. Der Designleitfaden bietet einen Überblick über die einzelnen Komponenten.

Tabella 5. Lösungskomponenten

VSPEX-Ebene	Komponenten
Anwendungsebene	VMware Horizon View 6.0-Desktopvirtualisierungsbroker mit: • View Manager • View Composer • View Persona Management • VMware Horizon View Storage Accelerator • VMware vCenter Operations Manager for Horizon View • VMware Horizon Workspace
Virtualisierungsebene	VMware vSphere-Hypervisor mit: • VMware vSphere • VMware vCenter-Server • VMware vSphere High Availability • vShield Endpoint
Datenverarbeitungsebene	VSPEX definiert die Mindestanzahl der auf der Rechnerebene benötigten Ressourcen, ermöglicht dem Benutzer jedoch, diese auf jeder Serverhardware zu implementieren, die diese Anforderungen erfüllt.
Netzwerkebene	VSPEX definiert die Mindestanzahl der für die Lösung erforderlichen Netzwerkports und bietet allgemeine Anweisungen zur Netzwerkarchitektur, ermöglicht dem Kunden jedoch, die Lösung mit beliebiger Netzwerkhardware zu implementieren, die diese Anforderungen erfüllt.
Speicherebene	EMC VNXe-Serie mit: • EMC Unisphere® Management Suite • EMC VSI for VMware vSphere Web Client • VMware vSphere Storage APIs for Array Integration (VAAI) • VMware vSphere Storage APIs for Storage Awareness • EMC VNXe Snapshots • EMC VNXe Virtual Provisioning™ • EMC FAST Suite – FAST Cache und Fully Automated Storage Tiering for Virtual Pools (FAST VP)
Datensicherheitsebene	EMC Avamar
Sicherheitsschicht	RSA SecurID

Kapitel 4 Lösungsimplementierung

In diesem Kapitel werden folgende Themen behandelt:

Überblick 24
Vorbereiten der Netzwerkinfrastruktur 25
Vorbereiten und Konfigurieren des Speicherarrays 27
Installation und Konfiguration der VMware vSphere-Hosts 36
Installation und Konfiguration der SQL Server-Datenbank 38
Bereitstellen von VMware vCenter Server 40
Einrichten von VMware Horizon View Connection Server 41
Provisioning von virtuellen Desktops 45
Einrichten von EMC Avamar 46
Einrichten von VMware vShield Endpoint 47
Einrichten von VMware Horizon Workspace 49
Einrichten von VMware vCenter Operations Manager for Horizon View 54

Überblick

In diesem Kapitel wird beschrieben, wie Sie die Referenzarchitekturen der Anwender-Computing-Lösung implementieren. Wenn Sie bereits über eine VSPEX Proven Infrastructure-Umgebung verfügen, können Sie Abschnitte mit den bereits abgeschlossenen Schritten für die Implementierung außer Acht lassen. Andernfalls finden Sie Informationen zur Konfiguration der erforderlichen Infrastrukturkomponenten im Proven Infrastructure-Leitfaden.

Hinweis: Diese Lösung erfordert bestimmte Infrastrukturservices, wie in Abbildung 3 auf Seite 21 gezeigt. Diese können auch von einer vorhandenen Infrastruktur am Kundenstandort, von einer VSPEX Private Cloud oder als dedizierte Ressourcen als Teil dieser Lösung bereitgestellt werden.

In Tabella 6 listet die Hauptphasen des Prozesses für die Implementierung der Lösung auf und enthält Links zu den relevanten Abschnitten in diesem Kapitel.

Tabella 6. Überblick über den Implementierungsprozess

Bereit-stellen	Beschreibung	Referenz
1	Konfigurieren der Switche und Netzwerke, Verbinden mit dem Kundennetzwerk	Vorbereiten der Netzwerkinfrastruktur auf Seite 25
2	Installieren und Konfigurieren der VNXe	Vorbereiten und Konfigurieren des Speicherarrays auf Seite 27
3	Konfigurieren der Datastores der virtuellen Maschinen	Vorbereiten und Konfigurieren des Speicherarrays auf Seite 27
4	Installieren und Konfigurieren der Server	Installation und Konfiguration der VMware vSphere-Hosts auf Seite 36
5	Einrichten von SQL Server (verwendet von vCenter und Horizon View)	Installation und Konfiguration der SQL Server-Datenbank auf Seite 38
6	Installieren und Konfigurieren von vCenter und des Netzwerks der virtuellen Maschine	Bereitstellen von VMware vCenter Server auf Seite 40
7	Einrichten von View Connection Server	Einrichten von VMware Horizon View Connection Server auf Seite 41
8	Einrichten von Avamar	Einrichten von EMC Avamar auf Seite 46
9	Einrichten von vShield Endpoint	Einrichten von VMware vShield Endpoint auf Seite 47
10	Einrichten von VMware Horizon Workspace	Einrichten von VMware Horizon Workspace auf Seite 49
11	Einrichten von vCenter Operations Manager for Horizon View	Einrichten von VMware vCenter Operations Manager for Horizon View auf Seite 54

Vorbereiten der Netzwerkinfrastruktur

In diesem Abschnitt werden die Anforderungen für die Vorbereitung der Netzwerkinfrastruktur beschrieben, die zum Support dieser Lösung erforderlich ist. In Tabella 7 enthält eine Zusammenfassung der abzuschließenden Aufgaben sowie Referenzen zur weiteren Information.

Tabella 7. Aufgaben für die Switch- und Netzwerkkonfiguration

Aufgabe	Beschreibung	Referenz
Konfigurieren der Netzwerkinfrastruktur	Konfigurieren Sie das Speicherarray und die vSphere-Hostnetzwerkinfrastruktur.	• Konfigurieren der Netzwerkinfra-struktur auf Seite 25
Konfigurieren der VLANs	Konfigurieren Sie private und öffentliche VLANs nach Bedarf.	• Konfigurieren der VLANs auf Seite 26 • Switch-Konfigurationsleitfaden Ihres Anbieters
Konfigurieren des Speichernetzwerks (nur FC)	Konfigurieren Sie die Fibre-Channel-Switchports, das Zoning für vSphere-Hosts und das Speicherarray.	• Konfigurieren des Speichernetzwerks (Blockvariante) auf Seite 26 • Switch-Konfigurationsleitfaden Ihres Anbieters
Abschließen der Netzwerkverkabelung	Verbinden Sie die Switchverbindungsports, VNXe-Ports und vSphere-Serverports.	• Vervollständigen der Netzwerkverka-belung auf Seite 27

Konfigurieren der Netzwerkinfra-struktur

Die Netzwerkinfrastruktur erfordert redundante Netzwerkverbindungen für jeden vSphere-Host, das Speicherarray, die Switchverbindungsports und die Switch-Uplink-Ports. Diese Konfiguration stellt sowohl Redundanz als auch zusätzliche Netzwerkbandbreite bereit.

Diese Konfiguration ist erforderlich, unabhängig davon, ob die Netzwerkinfrastruktur für die Lösung bereits vorhanden ist oder mit anderen Komponenten der Lösung bereitgestellt wird.

Abbildung 4 zeigt ein Beispiel einer redundanten Ethernet-Infrastruktur für diese Lösung. Hier ist die Nutzung von redundanten Switchen und Verbindungen dargestellt, um dafür zu sorgen, dass kein Single-Point-of-Failure in der Netzwerkverbindung vorhanden ist.

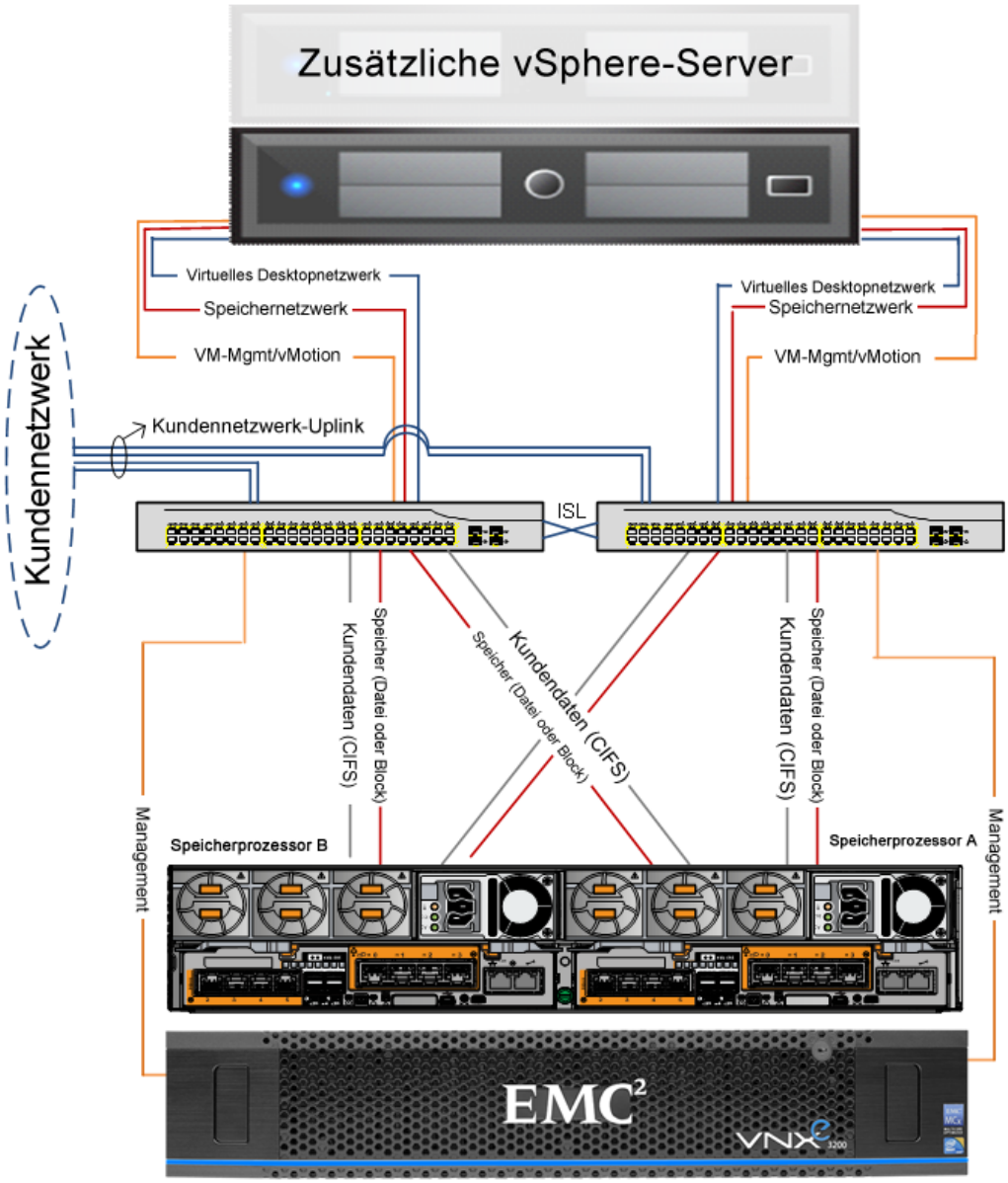


Abbildung 4. Beispiel-Ethernetnetzwerkarchitektur

Konfigurieren der VLANs

Achten Sie darauf, dass die Infrastruktur über geeignete Switchports für das Speicherarray und vSphere-Hosts verfügt. EMC empfiehlt, dass Sie die vSphere-Hosts mit mindestens 3 VLANs konfigurieren:

- **Clientzugriffsnetzwerk:** Virtuelles Maschinennetzwerk und Common Internet File System (CIFS)-Datenverkehr (kundenorientierte Netzwerke, die bei Bedarf getrennt werden können)
- **Speichernetzwerk**: NFS/iSCSI-Netzwerk (privates Netzwerk)
- **Managementnetzwerk:** vSphere-Management und VMware vMotion (privates Netzwerk)

Konfigurieren des Speichernetzwerks (Blockvariante)

Für die Blockvariante der Lösung ist ein separates Speichernetzwerk erforderlich. Für die FC-Netzwerkinfrastruktur sind redundante FC-Switche und Links für jeden vSphere-Host und das Speicherarray erforderlich. Diese Konfiguration stellt sowohl Redundanz als auch zusätzliche Speichernetzwerkbandbreite bereit.

Abbildung 5 zeigt ein Beispiel für ein FC-Netzwerk. Wir haben jeden vSphere-Host mit beiden FC-Switchen und jeden Switch mit jedem Speicherprozessor (SP) auf dem Speicherarray verbunden. Wir haben dann jede der Fibre-Channel-Verbindungen zwischen dem vSphere-Host und dem Speicher-Array in eine separate Fibre-Channel-Zone platziert.

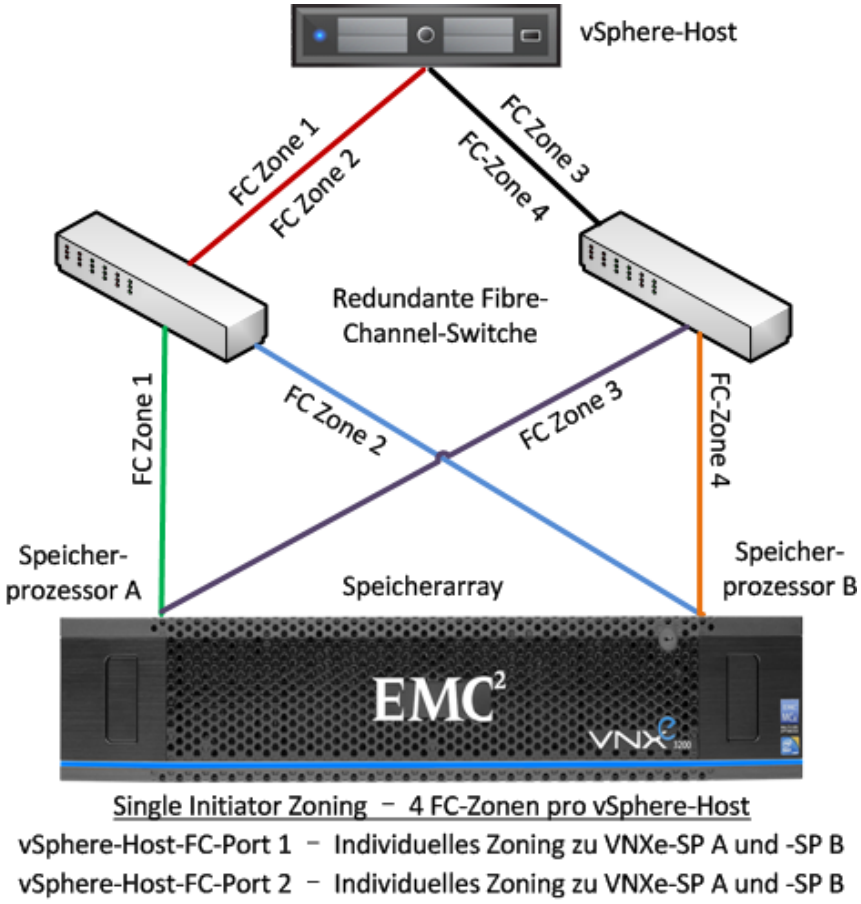


Abbildung 5. Beispiel für eine Fibre-Channel-Netzwerkarchitektur

Vervollständigen der Netzwerkverkabelung

Sorgen Sie dafür, dass alle Lösungsserver, Speicher-Arrays, Switch-Verbindungen und Switch Uplinks über redundante Verbindungen verfügen und in separate Switching-Infrastrukturen eingesteckt sind. Sorgen Sie dafür, dass die Speichernetzwerkinfrastruktur vollständig mit dem vorhandenen Kundennetzwerk verbunden ist.

Hinweis: Wenn die neue Ausrüstung mit dem vorhandenen Kundennetzwerk verbunden ist, achten Sie darauf, dass die Verbindung keine Serviceprobleme im Kundennetzwerk verursacht.

Vorbereiten und Konfigurieren des Speicherarrays

In diesem Abschnitt wird die Konfiguration des VNXe-Speicher-Arrays beschrieben. In dieser Lösung stellt die VNXe NFS- oder VMware Virtual Machine File System (VMFS)-Datenspeicher für VMware-Hosts bereit. In Tabella 8 zeigt die Aufgaben für die Speicherkonfiguration.

Tabella 8. Aufgaben für die Speicherkonfiguration

Aufgabe	Beschreibung	Referenz	
Vorbereiten der VNXe	Installieren Sie die VNXe-Hardware gemäß der Produktdokumentation.	VSPEX Private Cloud Proven Infrastructure-Leitfaden	
Einrichten der anfänglichen VNXe-Konfiguration	Konfigurieren Sie die IP-Adressinformationen und andere wichtige Parameter auf der VNXe.	Einrichten der anfänglichen VNXe-Konfiguration auf Seite 29 VSPEX Private Cloud Proven Infrastructure-Leitfaden	
Provisioning von Kerndatenspeicher	Konfigurieren Sie den Kerndatenspeicher so, wie es für die ausgewählte Lösungsvariante und -größe erforderlich ist.	Provisioning von Kerndatenspeicher auf Seite 29	*VNXe3200-Installationshandbuch* *Leitfaden für die ersten Schritte mit dem Unisphere-System* Konfigurationsleitfaden Ihres Switch-Anbieters Lösungsdesignleitfaden
Provisioning von Speicher für VMFS-Datastores (nur Block)	Erstellen Sie LUNs, die den vSphere-Servern als VMFS-Datastores angezeigt werden, die die virtuellen Desktops hosten. Aktivieren von FAST Cache	Provisioning von Speicher für VMFS-Datastores (nur Block) auf Seite 29	
Stellen Sie Speicher für NFS-Datastores (nur File) bereit.	Erstellen Sie NFS-Dateisysteme, die den vSphere-Servern als NFS-Datastores angezeigt werden, die die virtuellen Desktops hosten. Aktivieren von FAST Cache	Provisioning von Speicher für NFS-Datastores (nur Datei) auf Seite 31	
Konfigurieren Sie FAST Cache.	Konfigurieren Sie FAST Cache im Speicherpool.	Konfigurieren von FAST Cache auf Seite 33	
Provisioning von optionalem Speicher für Benutzerdaten	Erstellen Sie CIFS-Dateisysteme, die zum Speichern von Roaming-Benutzerprofilen und Stammverzeichnissen verwendet werden. Optional kann FAST VP konfiguriert werden.	Provisioning von optionalem Speicher für Benutzerdaten auf Seite 35	
Provisioning von optionalem Speicher für virtuelle Infrastruktur-maschinen	Erstellen Sie optional zusätzliche VMFS/NFS-Datastores zum Hosten von SQL Server, Domain-Controller, vCenter-Servern und virtuellen VMware Horizon View Connection Server-Maschinen.	Provisioning von optionalem Speicher für virtuelle Infrastrukturmaschinen auf Seite 35	
Konfigurieren der Schwellenwerte und Warnmeldungen für Virtual Provisioning	Konfigurieren Sie Schwellenwerte und damit verbundene Warnmeldungen für die Speicherpoolkapazität.	Festlegen der Schwellenwerte und Warnmeldungen für Virtual Provisioning auf Seite 36	

Vorbereiten der VNXe

Für diese Lösung sind keine spezifischen VNXe-Einrichtungsschritte erforderlich. Anweisungen für Zusammenstellung, Rackeinbau, Verkabelung und Stromversorgung des VNXe-Arrays finden Sie im *EMC VNXe3200-Installationshandbuch*.

Einrichten der anfänglichen VNXe-Konfiguration

Konfigurieren Sie nach der Vorbereitung der VNXe wichtige Informationen zur vorhandenen Umgebung, damit das Speicherarray mit ihr kommunizieren kann. Konfigurieren Sie die folgenden allgemeinen Elemente gemäß den für Ihr IT-Rechenzentrum geltenden Richtlinien und vorhandenen Infrastrukturinformationen.

- Domain Name System (DNS)
- Network Time Protocol (NTP)
- Schnittstellen des Speichernetzwerks
- IP-Adresse des Speichernetzwerks
- CIFS-Services und Active Directory-Domain-Mitgliedschaft

Weitere Informationen zum Konfigurieren der VNXe-Plattform finden Sie in den in Tabella 8 aufgelisteten Referenzdokumenten. Informationen zum Laufwerkslayout finden Sie im Designleitfaden.

Aktivieren von Jumbo Frames an den VNXe-Speichernetzwerkschnittstellen

Verwenden Sie Jumbo Frames für Speichernetzwerke, um mehr Netzwerkbandbreite zuzulassen, indem Sie die MTU-Größe wie angegeben über alle Netzwerkschnittstellen in der Umgebung anwenden:

1. Klicken Sie in Unisphere auf **Settings** › **More Configuration** › **Port Settings**.
2. Wählen Sie unter **IO Modules** Netzwerkschnittstellen aus.
3. Legen Sie die Option **MTU** auf **9.000** fest.
4. Klicken Sie auf **Apply**.

Erstellen der Linkzusammenfassungen auf den VNXe-Speichernetzwerkschnittstellen

Die Linkzusammenfassung sorgt für Netzwerkredundanz auf dem VNXe3200-System. Führen Sie zum Erstellen einer Netzwerkschnittstellen-Linkzusammenfassung die folgenden Schritte aus:

1. Wählen Sie unter **IO Modules** eine Netzwerkschnittstelle aus.
2. Wählen Sie **Aggregate with another network interface** aus.
3. Klicken Sie auf **Create Aggregation**.
4. Klicken Sie auf **Yes**, um die Änderungen zu übernehmen.

Provisioning von Kerndatenspeicher

Informationen zur Konfiguration des Kerndatenspeichers finden Sie im Designleitfaden, in dem das Zielspeicherlayout für die Block- und die File-Variante für 500 virtuelle Desktops beschrieben wird.

Provisioning von Speicher für VMFS-Datastores (nur Block)

Führen Sie die folgenden Schritte in Unisphere aus, um LUNs zum Speichern der virtuellen Desktops auf der VNXe zu konfigurieren:

1. Erstellen Sie einen blockbasierten RAID-5-Speicherpool mit den im Designleitfaden angegebenen Merkmalen.
   a. Melden Sie sich bei Unisphere an.
   b. Wählen Sie **Storage** › **Storage Configuration** › **Storage Pools**.
   c. Klicken Sie auf **List View**.
   d. Klicken Sie auf **Create**.
   e. Geben Sie im Dialogfeld die Poolparameter an und klicken Sie dann auf **OK**.
   f. Achten Sie darauf, dass FAST Cache für den Speicherpool aktiviert ist, wie in Abbildung 6 gezeigt.

Storage Pool Wizard
FAST Cache
Step 4 of 6
>>
The FAST Cache exists on the system. Each storage pool can be configured to use the FAST Cache. The FAST Cache is shared by all storage pools configured to use it.
Do you want this storage pool to use the FAST Cache?
Yes
No
< Back
Next >
Finish
Cancel
Help

Abbildung 6. Assistent für Speicherpools: FAST Cache

2. Konfigurieren Sie die erforderlichen LUNs aus dem Pool, wie im Designleitfaden dargestellt, um den vSphere-Servern 5 VMFS-Datastores anzuzeigen.
   a. Wählen Sie **Storage** › **VMware Datastores** aus.
   b. Klicken Sie auf **Create**.
   c. Wählen Sie **Datastore Type** (**VMFS**) aus.

d. Geben Sie unter **Datastore Name** einen Namen für den Datastore ein.

e. Wählen Sie den in Schritt 1 erstellten Pool aus und geben Sie die LUN-Größe sowie die Anzahl der bereitzustellenden LUNs an, wie im Designleitfaden beschrieben.

f. Konfigurieren Sie die Snapshot-Planung über die Option **Snapshot Schedule**.

g. Konfigurieren Sie den Hostzugriff für jeden Host über die Option **Host Access**.

h. Überprüfen Sie die Datastore-Konfiguration unter **Summary of DataStore Configuration** und klicken Sie auf **Finish**, um die Datastores zu erstellen.

i. Wiederholen Sie die obigen Schritte, bis Sie 4 weitere Datastores erstellt haben.

Provisioning von Speicher für NFS-Datastores (nur Datei)

Führen Sie die folgenden Schritte in Unisphere aus, um NFS-Dateisysteme auf der VNXe zum Speichern der virtuellen Desktops zu erstellen:

1. Erstellen Sie einen NAS-Server.

Hinweis: Eine Netzwerkschnittstelle ist einem NFS-Export zugeordnet. Dateifreigaben stellen Zugriff über diese Schnittstelle bereit.

a. Melden Sie sich bei der VNXe an.

b. Klicken Sie auf **Settings** › **NAS Servers**.

c. Klicken Sie auf **Create**.

d. Führen Sie im **NAS Server Wizard**, der in Abbildung 7 gezeigt ist, die folgenden Schritte aus:

i. Geben Sie unter **Server Name** einen Namen für den Server ein.

ii. Wählen Sie unter **Storage Pool** den Speicherpool aus, der die Dateifreigabe bereitstellen wird.

iii. Geben Sie unter **IP Address** die IP-Adresse für die Schnittstelle ein.

iv. Geben Sie unter **Subnet Mask/Prefix Length** die Subnetzmaske für die Schnittstelle ein.

v. Geben Sie unter **Gateway** die Gatewayadresse für die Schnittstelle ein.

vi. Klicken Sie auf **Erweiterte Funktionen**.

vii. Wählen Sie unter **Storage Processor** einen SP aus, der die Dateifreigabe unterstützt.

viii. Wählen Sie unter **Ethernet Port** den Ethernetport zu der Schnittstelle mit Linkzusammenfassung aus, die Sie unter Erstellen der Linkzusammenfassungen auf den VNXe-Speichernetzwerkschnittstellen auf Seite 29 erstellt haben.

ix. Geben Sie unter **VLAN ID** die VLAN-ID an, falls diese erforderlich ist.

x. Klicken Sie auf **Next**.

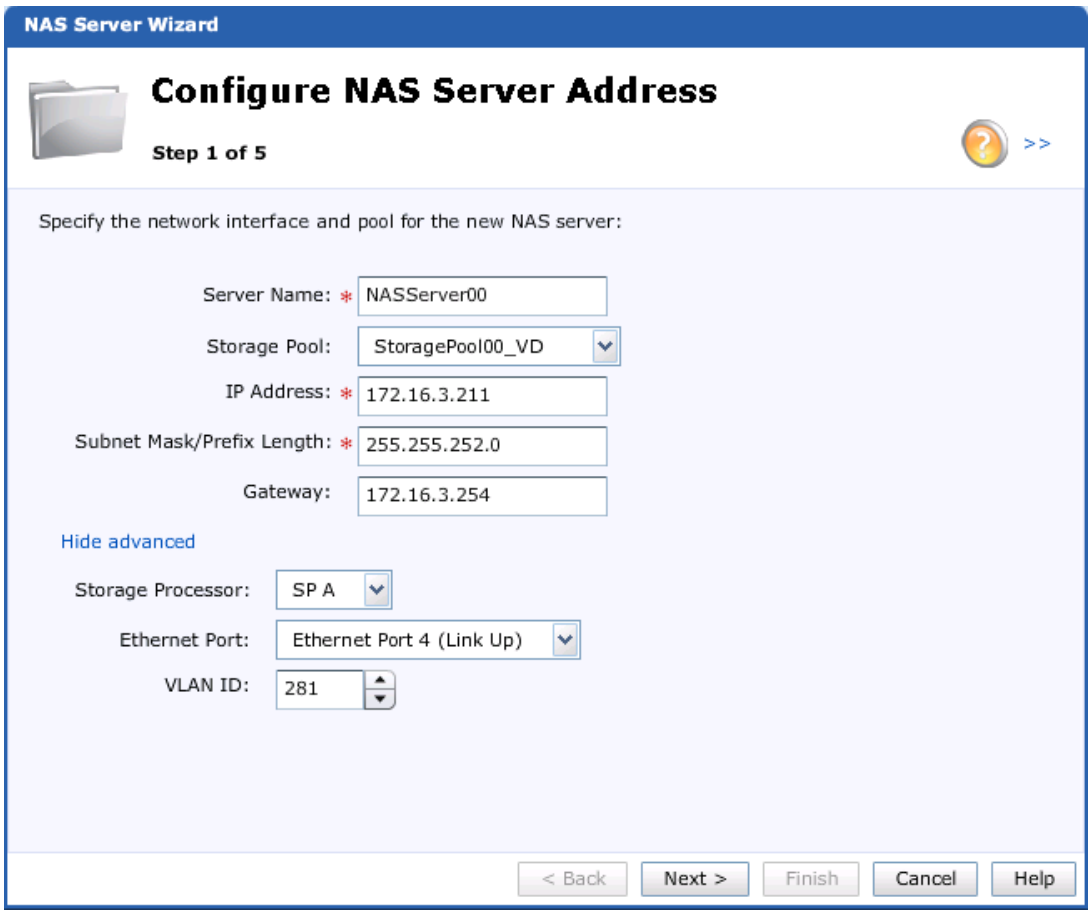


Abbildung 7. Konfigurieren der NAS-Serveradresse über das entsprechende Dialogfeld

xi. Wählen Sie **Linux/Unix shares (NFS)** aus.

xii. Geben Sie den **DNS/NIS** ein, falls erforderlich.

xiii. Überprüfen Sie die Zusammenfassung unter **NAS Server Summary** und klicken Sie auf **Finish**.

2. Erstellen Sie einen RAID-5-Speicherpool mit den im Designleitfaden angegebenen Merkmalen.

   a. Melden Sie sich bei Unisphere an.

   b. Wählen Sie **Storage** › **Storage Configuration** › **Storage Pools**.

   c. Klicken Sie auf **List View**.

   d. Klicken Sie auf **Create**.

   e. Geben Sie im Dialogfeld die Poolparameter an und klicken Sie dann auf **OK**.

   f. Achten Sie darauf, dass FAST Cache für den Pool aktiviert ist.

3. Konfigurieren Sie die erforderlichen Datastores aus dem Pool, wie im Designleitfaden dargestellt, um den vSphere-Servern 5 NFS-Datastores anzuzeigen.

   a. Wählen Sie **Storage** › **VMware Datastores** aus.

   b. Klicken Sie auf **Create**.

c. Wählen Sie **Datastore Type (NFS)** aus.

d. Geben Sie unter **Datastore Name** einen Namen für den Datastore ein.

e. Wählen Sie den in Schritt 2 erstellten Pool aus und geben Sie die Datastore-Größe sowie die Anzahl der bereitzustellenden Datastores an, wie im Designleitfaden beschrieben.

f. Konfigurieren Sie die **Snapshot-Planung**.

g. Konfigurieren Sie den Hostzugriff für jeden Host über die Option **Host Access**.

h. Überprüfen Sie die Datastore-Konfiguration unter **Summary of DataStore Configuration** und klicken Sie auf **Finish**, um die Datastores zu erstellen.

i. Wiederholen Sie die obigen Schritte, bis Sie 4 weitere Datastores erstellt haben.

Konfigurieren von FAST Cache

Führen Sie die folgenden Schritte in Unisphere aus, um FAST Cache auf dem Speicherpool für diese Lösung zu konfigurieren.

1. Erstellen Sie FAST-Cache:

   a. Klicken Sie auf **Storage › Storage Configuration › Fast Cache.**

   b. Klicken Sie auf **Create**, um den Konfigurationsassistenten zu starten.

   Der Assistent zeigt an, ob das System für die Verwendung der FAST Cache-Funktion lizenziert ist und über berechtigte Flashlaufwerke verfügt.

   c. Klicken Sie auf **Next**.

   Der Assistent zeigt die Anzahl der Festplatten und den RAID-Typ an.

   d. Klicken Sie auf **Finish**, um die Konfiguration abzuschließen.

   Der Bildschirm **Results** wird angezeigt, wie in Abbildung 8 dargestellt.

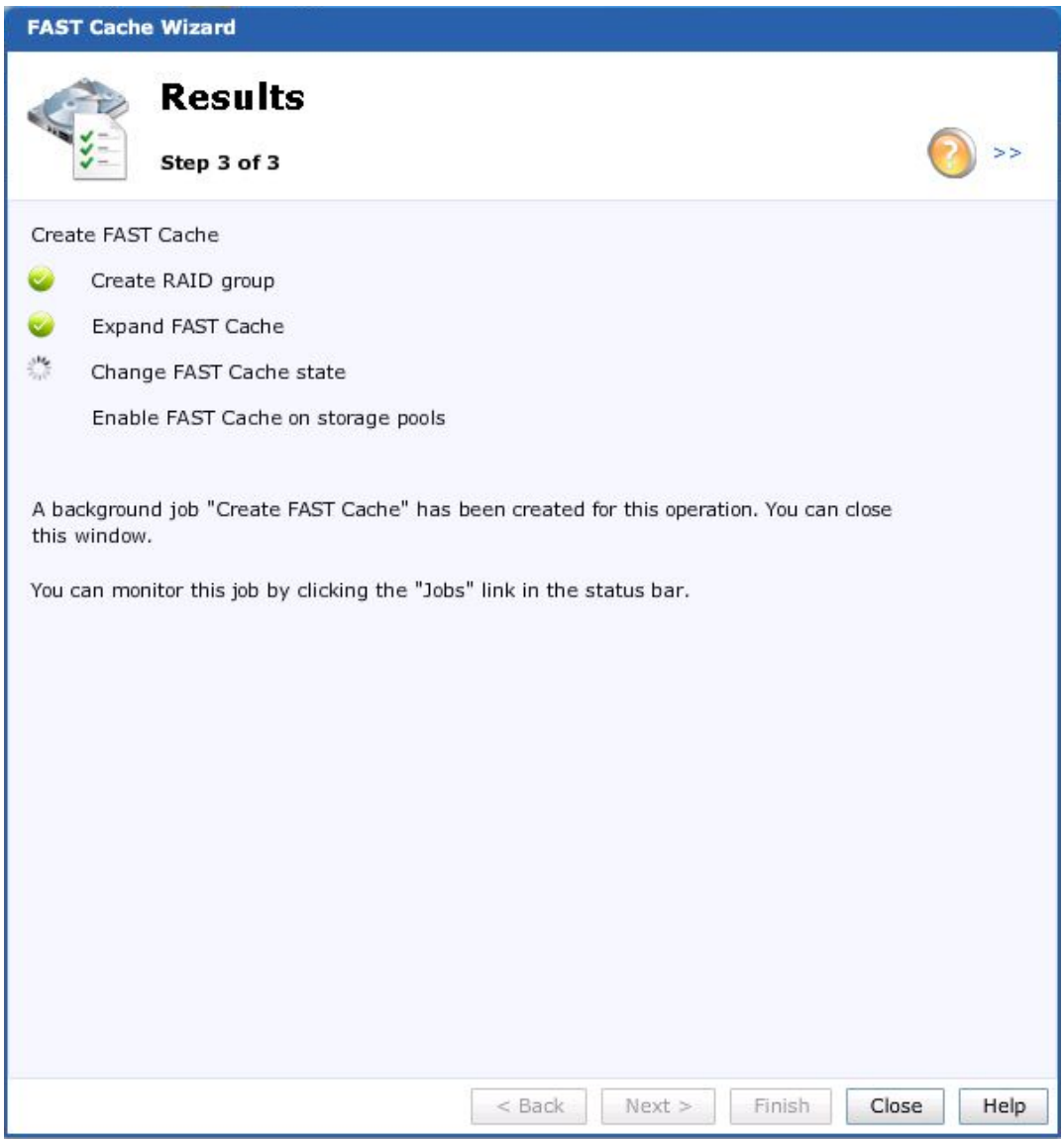

FAST Cache Wizard
Results
Step 3 of 3
>>
Create FAST Cache
Create RAID group
Expand FAST Cache
Change FAST Cache state
Enable FAST Cache on storage pools
A background job "Create FAST Cache" has been created for this operation. You can close this window.
You can monitor this job by clicking the "Jobs" link in the status bar.
< Back
Next >
Finish
Close
Help

Abbildung 8. FAST Cache-Assistent: Ergebnisbildschirm

e. Klicken Sie auf **Next**.

> **Hinweis**: Wenn keine ausreichende Anzahl von Flashlaufwerken vorhanden ist, steht die Option **Next** nicht zur Verfügung.

2. Aktivieren Sie FAST Cache im Speicherpool.

   Wenn eine LUN in einem Speicherpool erstellt wird, können Sie FAST Cache nur für die LUN auf der Speicherpoolebene konfigurieren. FAST Cache ist bei allen in dem Speicherpool erstellten LUNs aktiviert oder deaktiviert. Sie haben FAST Cache aktiviert, als Sie den Speicherpool mit den voranstehenden Anweisungen erstellten.

   Wählen Sie den Speicherpool aus und klicken Sie dann auf **Details**. Unter **Settings** konfigurieren Sie FAST Cache wie gezeigt in Abbildung 9.

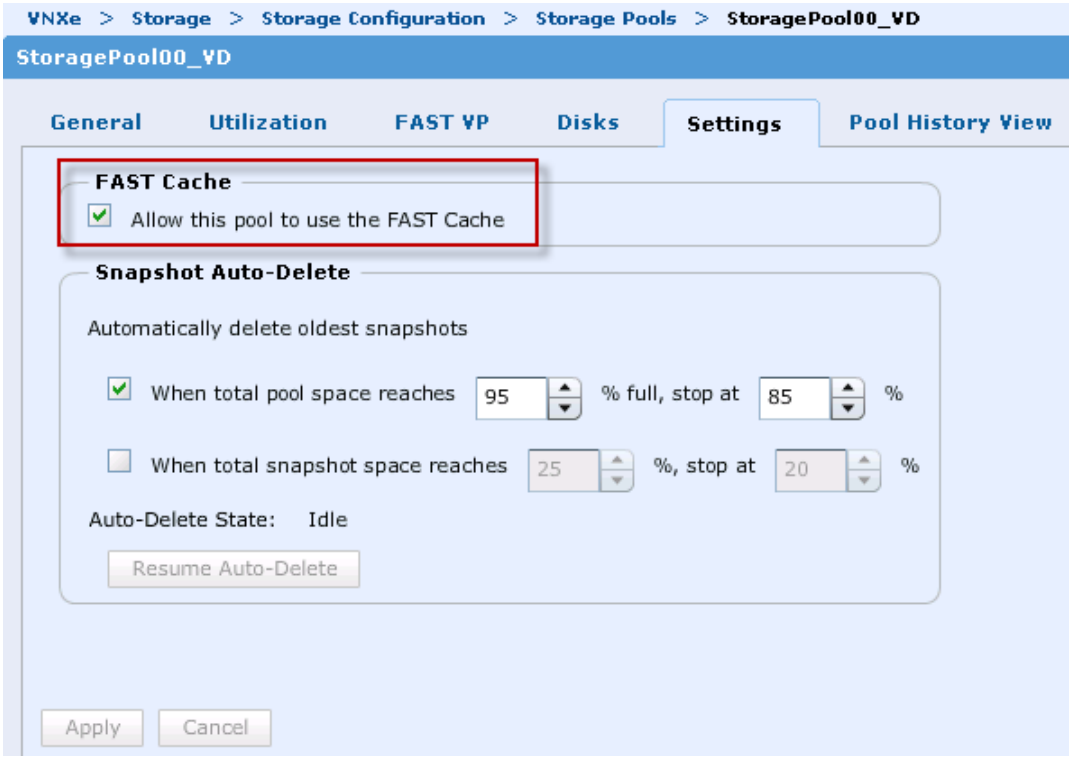


Abbildung 9. Registerkarte „Advanced“ im Dialogfeld „Storage Pool Properties“

Hinweis: Die FAST Cache-Funktion auf der VNXe führt nicht zu einer sofortigen Performanceverbesserung. Das System muss Daten zu Zugriffsmustern sammeln und häufig verwendete Informationen in den Cache hochstufen. Dieser Prozess kann einige Stunden dauern, in denen sich die Performance des Arrays kontinuierlich verbessert.

Provisioning von optionalem Speicher für Benutzerdaten

Wenn in der Produktionsumgebung noch kein für Benutzerdaten (das heißt Roamingbenutzerprofile oder View Persona Management Repositories und Stammverzeichnisse) erforderlicher Speicher vorhanden ist und die optionale Benutzerdatenspindel erworben wurde, führen Sie die folgenden Schritte in Unisphere aus, um 2 CIFS-Dateisysteme auf der VNXe zu erstellen:

1. Erstellen Sie einen RAID-5-Speicherpool mit den im Designleitfaden angegebenen Merkmalen.
2. Stellen Sie 2 CIFS-Shares auf einem CIFS-Server bereit, wie im Designleitfaden angegeben.

Provisioning von optionalem Speicher für virtuelle Infrastruktur-maschinen

Wenn der für virtuelle Infrastrukturmaschinen (das heißt SQL Server, Domain-Controller, vCenter-Server und Horizon View Connection-Server) erforderliche Speicher in der Produktionsumgebung noch nicht vorhanden ist und die optionale Benutzerdatenspindel erworben wurde, konfigurieren Sie ein NFS-Dateisystem auf der VNXe, das als NFS-Datastore verwendet wird, in dem sich die virtuellen Infrastrukturmaschinen befinden. Wiederholen Sie die in Provisioning von Speicher für NFS-Datastores (nur Datei) auf Seite 31 gezeigten Konfigurationsschritte, um den optionalen Speicher bereitzustellen, und berücksichtigen Sie dabei die kleinere Anzahl von Laufwerken.

Festlegen der Schwellenwerte und Warnmeldungen für Virtual Provisioning

Zum Festlegen von Kapazitäts-Schwellenwertwarnmeldungen für einen bestimmten Pool führen Sie die folgenden Schritte aus:

1. Wählen Sie den Pool aus und klicken Sie auf **Details**.
2. Legen Sie unter **Utilization** die Option **Alert Threshold** für den Pool fest, wie in Abbildung 10 gezeigt.

   Used Space, **Available Space** und **Subscription** sind wichtige Kennzahlen, die Sie untersuchen sollten.

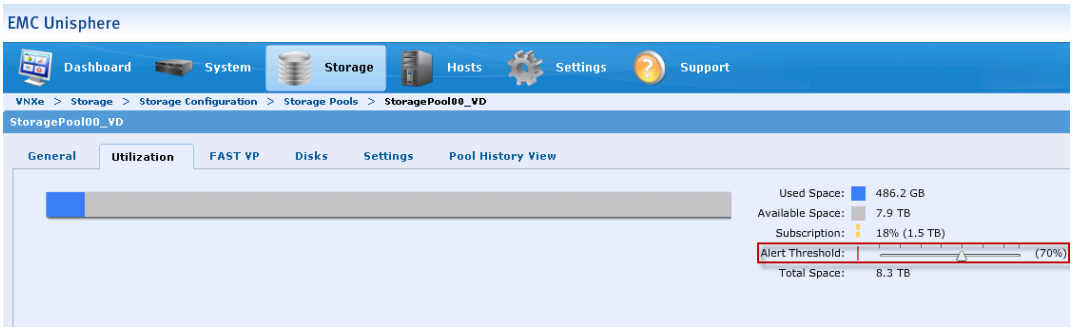


Abbildung 10. Definieren der Schwellenwerte für die Speicherpoolauslastung

Zusätzlichen Einstellungen, die für das Speicherplatzmanagement relevant sind, sind unter „Settings“ zu finden, wie in Abbildung 11 gezeigt. **Snapshot Auto-Delete**-Einstellungen sollten aktiviert werden, wenn die Snapshot-Funktion verwendet wird.

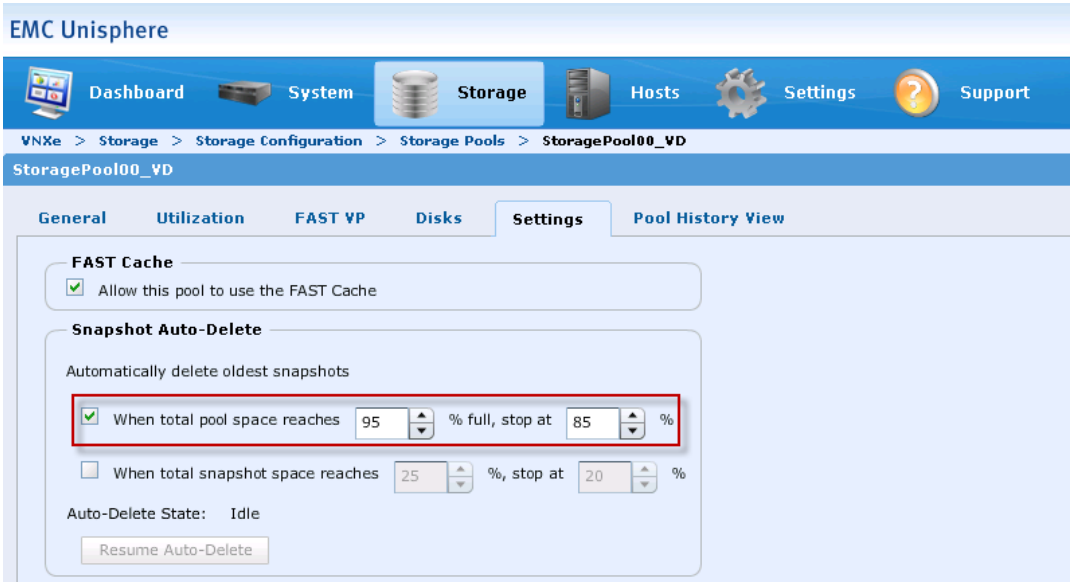


Abbildung 11. Snapshot-Einstellungen für Speicherpools

Installation und Konfiguration der VMware vSphere-Hosts

In diesem Abschnitt werden Informationen zur Installation und Konfiguration der vSphere-Hosts und Infrastrukturserver bereitgestellt, die für den Support der Architektur erforderlich sind. In Tabella 9 beschreibt die Aufgaben, die abgeschlossen werden müssen.

Tabella 9. Aufgaben für die Serverinstallation

Aufgabe	Beschreibung	Referenz
Installieren von vSphere	Installieren Sie den vSphere-Hypervisor auf den physischen Servern, die für die Lösung bereitgestellt werden.	• Installieren von vSphere auf Seite 37 • *Installations- und Einrichtungshandbuch für vSphere*
Konfigurieren des vSphere-Netzwerks	Konfigurieren Sie das vSphere-Netzwerk, einschließlich NIC-Trunking, VMkernel-Ports, Portgruppen für virtuelle Maschinen und Jumbo Frames.	• Konfigurieren des vSphere-Netzwerks auf Seite 37 • *Handbuch für vSphere-Netzwerk*
Verbinden der VMware-Datastores	Verbinden Sie die VMware-Datastores mit den für die Lösung bereitgestellten vSphere-Hosts.	• Verbinden der VMware-Datastores auf Seite 38 • *Handbuch für vSphere-Speicher*

Installieren von vSphere

Bestätigen oder aktivieren Sie nach dem ersten Einschalten der für vSphere verwendeten Server die Einstellung für die hardwaregestützte CPU-Virtualisierung und die hardwaregestützte MMU-Virtualisierung im BIOS des Servers. Wenn die Server mit einem RAID-Controller ausgestattet sind, empfiehlt EMC, eine Spiegelung auf den lokalen Festplatten zu konfigurieren.

Starten Sie die vSphere-Installationsmedien, und installieren Sie den Hypervisor auf jedem der Server. Für die Installation sind vSphere-Hostnamen, IP-Adressen und ein Root-Passwort erforderlich. In Arbeitsblatt für die Kundenkonfiguration auf Seite 66 finden Sie die entsprechenden Werte.

Konfigurieren des vSphere-Netzwerks

Im Handbuch für VMware *vSphere-Netzwerk* wird die vSphere-Netzwerkkonfiguration beschrieben, einschließlich Lastenausgleich, Linkzusammenfassung und Failover-Optionen. Wählen Sie die entsprechende Option für den Lastenausgleich auf der Basis dessen aus, was von der Netzwerkinfrastruktur unterstützt wird. Weitere Informationen finden Sie in der Liste von Dokumenten in Kapitel 6, Referenzdokumentation auf Seite 61.

Netzwerkschnittstellenkarten

Während der Installation von vSphere wird ein virtueller Standard-Switch (vSwitch) erstellt. Standardmäßig wählt vSphere nur eine physische NIC als virtuellen Switch Uplink aus. Zum Erfüllen der Redundanz- und Bandbreitenanforderungen konfigurieren Sie eine zusätzliche NIC, entweder über die vSphere-Konsole oder durch eine Verbindung mit dem vSphere-Host vom vSphere-Client aus.

Jeder vSphere-Server sollte über mehrere NICs für jedes virtuelle Netzwerk verfügen, um Redundanz und die Verwendung von Netzwerklastenausgleich, Link-Zusammenfassung und Netzwerkadapter-Failover zu ermöglichen.

VMkernel-Ports

Erstellen Sie VMkernel-Ports nach Bedarf, basierend auf der Infrastrukturkonfiguration:

- VMkernel-Port für NFS-Datenverkehr (nur File-Variante)

- VMkernel-Port für vMotion
- Virtuelle Desktop-Portgruppen (verwendet von den virtuellen Desktops für die Kommunikation im Netzwerk)

Im *Handbuch für vSphere-Netzwerk* wird das Verfahren für die Konfiguration dieser Einstellungen beschrieben.

Jumbo Frames

Sie können Jumbo Frames auf dem vSphere-Server in 2 verschiedenen Stufen aktivieren:

- Wenn für alle Ports auf dem vSwitch Jumbo Frames aktiviert werden sollen, bearbeiten Sie die MTU-Einstellungen unter **Properties** für den vSwitch in vCenter.
- Wenn Jumbo Frames für bestimmte VMkernel-Ports aktiviert werden sollen, bearbeiten Sie den VMkernel-Port unter **Network Properties** in vCenter.

Darüber hinaus müssen Jumbo Frames möglicherweise auf jedem Netzwerkswitch aktiviert werden. Anweisungen dazu finden Sie im Konfigurationsleitfaden für Ihren Switch.

Verbinden der VMware-Datastores

Verbinden Sie die in Vorbereiten und Konfigurieren des Speicherarrays auf Seite 27 konfigurierten Datastores mit den entsprechenden vSphere-Servern. Dazu zählen die Datastores, die für die folgenden Zwecke konfiguriert wurden:

- Virtueller Desktop-Speicher
- Virtueller Infrastrukturmaschinenspeicher (falls erforderlich)
- SQL Server-Speicher (falls erforderlich)

Anweisungen zum Verbinden der VMware-Datastores mit dem vSphere-Host finden Sie im *Handbuch für vSphere-Speicher*.

Installation und Konfiguration der SQL Server-Datenbank

In Tabella 10 beschreibt die Aufgaben für die Einrichtung und Konfiguration einer Microsoft SQL Server-Datenbank für die Lösung. Wenn die Aufgaben abgeschlossen sind, ist SQL Server auf einer virtuellen Maschine eingerichtet und alle für vCenter, Update Manager, Horizon View und View Composer erforderlichen Datenbanken sind zur Verwendung konfiguriert.

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für die virtuelle SQL Server-Maschine in den Pool der EMC VSPEX Private Cloud zu integrieren. Die empfohlenen Werte für CPU und Arbeitsspeicher sind 2 beziehungsweise 6 GB.

Tabella 10. Aufgaben für die SQL Server-Datenbankkonfiguration

Aufgabe	Beschreibung	Referenz
Erstellen einer virtuellen Maschine für SQL Server	Erstellen Sie eine virtuelle Maschine zum Hosten von SQL Server auf einem der vSphere-Server, der für virtuelle Infrastrukturmaschinen vorgesehen ist, und verwenden Sie den für die gemeinsame Infrastruktur designierten Datastore. Überprüfen Sie, ob der virtuelle Server die Hardware- und Softwareanforderungen erfüllt.	*vSphere-Administratorhandbuch für virtuelle Maschinen*
Installieren von Windows	Installieren Sie Microsoft Windows Server 2012 R2 Standard Edition auf der virtuellen Maschine.	*Installieren von Windows Server 2012 R2*
Installieren von SQL Server	Installieren Sie Microsoft SQL Server auf der virtuellen Maschine.	*Installieren von SQL Server (SQL Server 2012)*
Konfigurieren der Datenbank für vCenter Server	Erstellen Sie die für vCenter Server erforderliche Datenbank auf dem entsprechenden Datastore.	*Vorbereiten der vCenter Server-Datenbanken*
Konfigurieren der Datenbank für Update Manager	Erstellen Sie die für VMware Update Manager erforderliche Datenbank auf dem entsprechenden Datastore.	*Vorbereiten der Update Manager-Datenbank*
Konfigurieren der Datenbank für Horizon View Composer	Erstellen Sie die für VMware Horizon View Composer erforderliche Datenbank auf dem entsprechenden Datastore.	*Installation von VMware Horizon View*
Konfigurieren der Datenbank für Horizon View Manager	Erstellen Sie die für die VMware Horizon View Manager-Ereignisprotokolle erforderliche Datenbank auf dem entsprechenden Datastore.	*Installation von VMware Horizon View*
Konfigurieren der Datenbankberech-tigungen für Horizon View und View Composer	Konfigurieren Sie den Datenbankserver mit den entsprechenden Berechtigungen für die Horizon View- und Horizon View Composer-Datenbanken.	*Installation von VMware Horizon View*
Konfigurieren der vCenter-Datenbankberech-tigungen	Konfigurieren Sie den Datenbankserver mit den entsprechenden Berechtigungen für vCenter.	*Vorbereiten der vCenter Server-Datenbanken*
Konfigurieren der Update Manager-Datenbankberech-tigungen	Konfigurieren Sie den Datenbankserver mit den entsprechenden Berechtigungen für Update Manager.	*Vorbereiten der Update Manager-Datenbank*

Bereitstellen von VMware vCenter Server

In Tabella 11 beschreibt die Aufgaben, die für die Konfiguration von vCenter Server für die Lösung erforderlich sind.

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für die virtuelle vCenter Server-Maschine in den Pool der EMC VSPEX Private Cloud zu integrieren. Die empfohlenen Werte für CPU und Arbeitsspeicher sind 4 beziehungsweise 8 GB.

Tabella 11. Aufgaben für die vCenter-Konfiguration

Aufgabe	Beschreibung	Referenz
Erstellen Sie die virtuelle vCenter-Hostmaschine.	Erstellen Sie eine virtuelle Maschine für vCenter Server.	*vSphere-Administratorhandbuch für virtuelle Maschinen*
Installieren des vCenter-Gastbetriebssystems	Installieren Sie Windows Server 2012 R2 Standard Edition auf der virtuellen vCenter-Hostmaschine.	VMware vSphere-Dokumentation
Aktualisieren Sie die virtuelle Maschine.	Installieren Sie VMware Tools, aktivieren Sie die Hardwarebeschleunigung, und gewähren Sie den Remotezugriff auf die Konsole.	*vSphere-Administratorhandbuch für virtuelle Maschinen*
Erstellen von vCenter ODBC-Verbindungen	Erstellen Sie die 64-Bit vCenter und 32-Bit vCenter Update Manager ODBC-Verbindungen.	• *Installations- und Einrichtungshandbuch für vSphere* • *Installieren und Verwalten von VMware vSphere Update Manager*
Installieren Sie vCenter Server.	Installieren Sie die vCenter Server-Software.	*Installations- und Einrichtungshandbuch für vSphere*
Installieren Sie vCenter Update Manager.	Installieren Sie die vCenter Update Manager-Software.	*Installieren und Verwalten von VMware vSphere Update Manager*
Erstellen Sie ein virtuelles Rechenzentrum.	Erstellen Sie ein virtuelles Rechenzentrum.	*Handbuch für vCenter Server- und Hostverwaltung*
Wenden Sie die vSphere-Lizenzschlüssel an.	Geben Sie die vSphere-Lizenzschlüssel in das vCenter-Lizenzierungsmenü ein.	*Installations- und Einrichtungshandbuch für vSphere*
Fügen Sie vSphere-Hosts hinzu.	Verbinden Sie den vCenter-Server mit den vSphere-Hosts.	*Handbuch für vCenter Server- und Hostverwaltung*
Konfigurieren Sie vSphere-Clustering.	Erstellen Sie ein vSphere-Cluster, und verschieben Sie die vSphere-Hosts in das Cluster.	*Handbuch zur vSphere-Ressourcenverwaltung*

Aufgabe	Beschreibung	Referenz
Durchführen der vSphere-Hosterkennung vom Array	Führen Sie die vSphere-Hosterkennung von der Unisphere-Konsole durch.	*TechBook: Verwenden von EMC VNXe-Speicher mit VMware vSphere*
Installieren Sie das vCenter Update Manager-Plug-in.	Installieren Sie das vCenter Update Manager-Plug-in von der Administrationskonsole.	*Installieren und Verwalten von VMware vSphere Update Manager*
Bereitstellen des VAAI-Plug-ins	Stellen Sie mithilfe von Update Manager das VAAI-Plug-in für VNXe für alle vSphere-Hosts bereit.	• *EMC VNXe VAAI NFS-Plug-in – Readme-Datei* • *Installieren und Verwalten von VMware vSphere Update Manager*
Bereitstellen von PowerPath/VE (Blockvariante)	Stellen Sie mithilfe von Update Manager das PowerPath/VE-Plug-in für alle vSphere-Hosts bereit.	*Installations- und Administrationshandbuch für PowerPath/VE für VMware vSphere*
Installieren und Konfigurieren von EMC VSI für VMware vSphere Web Client OVA-Datei	Verwenden Sie den vSphere Web Client zur Installation des VSI für VMware vSphere Web Client OVA-Datei.	*EMC VSI für VMware vSphere Web Client – Produktleitfaden*
Installieren von EMC PowerPath Viewer (Blockvariante)	Installieren Sie PowerPath Viewer auf der Administrationskonsole.	*Installations- und Administrationshandbuch für EMC PowerPath Viewer*

Einrichten von VMware Horizon View Connection Server

In diesem Abschnitt finden Sie Informationen zum Einrichten und Konfigurieren von VMware Horizon View Connection Server für die Lösung. Für eine Neuinstallation von Horizon View empfiehlt VMware, dass Sie die Aufgaben in der in Tabella 12 angegebenen Reihenfolge durchführen.

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für die virtuellen View Connection Server-Maschinen in den Pool der EMC VSPEX Private Cloud zu integrieren. Die empfohlenen Werte für CPU und Arbeitsspeicher sind 2 beziehungsweise 5 GB.

Tabella 12. Aufgaben für die Einrichtung der VMware Horizon View-Verbindungsserver

Aufgabe	Beschreibung	Referenz	
Erstellen Sie virtuelle Maschinen für VMware Horizon View Connection Server.	Erstellen Sie zwei virtuelle Maschinen in vSphere Client. Diese virtuellen Maschinen werden als View Connection Server-Hosts verwendet. Installieren Sie Windows Server 2012 R2 als Gastbetriebssystem für diese Server.	Erstellen virtueller Maschinen für die VMware Horizon View Connection Server auf Seite 43	*Installation von VMware Horizon View*

Aufgabe	Beschreibung	Referenz	
Installieren Sie VMware Horizon View Connection Server.	Installieren Sie die View Connection Server-Software auf einer der zuvor vorbereiteten virtuellen Maschinen. Geben Sie den View-Lizenzschlüssel in die View Manager-Webkonsole ein.	Installieren von VMware Horizon View Connection Server auf Seite 43	
Konfigurieren der Verbindung zur View-Ereignisprotokolldatenbank	Konfigurieren Sie die Einstellungen für die View-Ereignisprotokolldatenbank mithilfe der entsprechenden Datenbankinformationen und Anmeldedaten.	Konfigurieren der Verbindung zur View-Ereignisprotokolldatenbank auf Seite 43	
Hinzufügen einer View Connection Server-Replikatinstanz	Installieren Sie die View Connection Server-Software auf dem zweiten Server.	Hinzufügen einer View Connection Server-Replikatinstanz auf Seite 43	
Konfigurieren der View Composer-ODBC-Verbindung	Konfigurieren Sie entweder auf dem vCenter-Server oder einem dedizierten Windows Server 2012 R2-Server eine ODBC-Verbindung für die zuvor konfigurierte View Composer-Datenbank.	Konfigurieren der View Composer-ODBC-Verbindung auf Seite 43	
Installieren von View Composer	Installieren Sie View Composer auf dem im vorherigen Schritt verwendeten Server.	Installieren von View Composer auf Seite 43	
Verbinden von VMware Horizon View mit vCenter und View Composer	Verbinden Sie Horizon View über die View Manager-Webbenutzeroberfläche mit dem vCenter-Server und View Composer.	Verbinden von VMware Horizon View mit vCenter und View Composer auf Seite 43	*Verwaltung von VMware Horizon View*
Bereiten Sie eine virtuelle Master-Maschine vor.	Erstellen Sie eine virtuelle Master-Maschine als Basis-Image für die virtuellen Desktops.	Vorbereiten einer virtuellen Master-Maschine auf Seite 44	
Konfigurieren von View Persona Management-Gruppen-Policies	Konfigurieren Sie Active Directory-Gruppen-Policies, um View Persona Management zu aktivieren.	Konfigurieren von View Persona Management-Gruppen-Policies auf Seite 44	
Konfigurieren von Gruppen-Policies für die Ordnerumleitung für EMC Avamar	Konfigurieren Sie Active Directory-Gruppen-Policies, um die Ordnerumleitung für Avamar zu aktivieren.	Konfigurieren von Gruppen-Policies für die Ordnerumleitung für EMC Avamar auf Seite 44	
Konfigurieren von View PCoIP-Gruppen-Policies	Konfigurieren Sie Active Directory-Gruppen-Policies für PCoIP-Protokolleinstellungen.	Konfigurieren von View PCoIP-Gruppen-Policies auf Seite 45	

Erstellen virtueller Maschinen für die VMware Horizon View Connection Server

Erstellen Sie in vSphere Client zwei virtuelle Maschinen, die als View Connection Server-Hosts verwendet werden, und installieren Sie Windows Server 2012 R2 als Gastbetriebssystem.

Installieren von VMware Horizon View Connection Server

Installieren Sie die View Connection Server-Software gemäß den Anweisungen in *Installation von VMware Horizon View*. Wählen Sie **Standard** aus, wenn Sie aufgefordert werden, den View-Verbindungsservertypen einzugeben. Geben Sie den View-Lizenzschlüssel in die View Manager-Adminkonsole ein.

Konfigurieren der Verbindung zur View-Ereignisproto-kolldatenbank

Konfigurieren Sie die Verbindung zur View-Ereignisprotokolldatenbank mithilfe des Datenbankservernamens, des Datenbanknamens und der Datenbankanmeldedaten. Spezifische Informationen zum Konfigurieren des Ereignisprotokolls finden Sie im Leitfaden zur *Installation von VMware Horizon View*.

Hinzufügen einer View Connection Server-Replikatinstanz

Wiederholen Sie den Installationsprozess für den View-Verbindungsserver auf der zweiten virtuellen Zielmaschine. Wenn Sie aufgefordert werden, den Verbindungsservertyp einzugeben, geben Sie **Replica** an, und stellen Sie dann die Anmeldedaten für den VMware Horizon View-Administrator bereit, um die View-Konfigurationsdaten von der ersten View Connection Server-Instanz zu replizieren.

Konfigurieren der View Composer-ODBC-Verbindung

Erstellen Sie auf dem Server, der den View Composer-Service hostet, eine ODBC-Verbindung für die zuvor konfigurierte View Composer-Datenbank. Spezifische Informationen zum Konfigurieren der ODBC-Verbindung finden Sie unter *Installation von VMware Horizon View*.

Installieren von View Composer

Installieren Sie die View Composer-Software auf dem Server, der den View Composer-Service hostet. Geben Sie auf Aufforderung während des Installationsprozesses die zuvor konfigurierte ODBC-Verbindung an. Spezifische Informationen zum Konfigurieren der ODBC-Verbindung finden Sie unter *Installation von VMware Horizon View*.

Verbinden von VMware Horizon View mit vCenter und View Composer

Erstellen Sie mithilfe der Horizon View Manager-Webkonsole die Verbindung zwischen Horizon View und dem vCenter-Server und View Composer. Spezifische Anweisungen zum Erstellen der Verbindungen finden Sie im Handbuch *Verwaltung von VMware Horizon View*. Wenn die Option zur Verfügung gestellt wird, aktivieren Sie das vSphere-Hostcaching (auch als View Storage Accelerator oder Content Based Read Cache bezeichnet) und legen Sie die Cachegröße auf 2 GB fest, die maximal unterstützte Größe.

Sie können darüber hinaus die Option **Reclaim VM disk space** aktivieren. Diese Funktion wird derzeit nur für Windows 8.1-Desktops unterstützt. Wenn Sie **Reclaim VM disk space** aktivieren, müssen Sie einen Inaktivitätszeitraum festlegen, mit dem gesteuert wird, wann der Vorgang nicht ausgeführt werden sollte. Da der Vorgang nicht in Phasen mit hoher Auslastung ausgeführt werden sollte, schließen Sie diese Zeiten in den Inaktivitätszeitraum ein. Standardmäßig wird die Speicherplatzrückgewinnung erst dann ausgeführt, wenn mindestens 1 GB Speicherplatz zurückgewonnen werden kann. Sie können während der Implementierung des Desktoppools einen anderen Wert angeben.

Vorbereiten einer virtuellen Master-Maschine

Führen Sie die folgenden Schritte aus, um die virtuelle Master-Maschine vorzubereiten:

1. Erstellen Sie mit dem vSphere-Webclient eine virtuelle Maschine auf der Grundlage der Hardwarespezifikationen für VMware Version 9.

   Sie können virtuelle Maschinen mit Version 9 nicht mit dem Softwareclient erstellen, sondern müssen den Webclient verwenden.

2. Installieren Sie das Windows 8.1-Gastbetriebssystem.
3. Installieren Sie entsprechende Integrationstools wie VMware Tools.
4. Optimieren Sie die Betriebssystemeinstellungen, um zu verhindern, dass unnötige Hintergrundservices irrelevante I/O-Vorgänge generieren, die sich negativ auf die allgemeine Performance des Speicherarrays auswirken.

   Ausführliche Informationen finden Sie in den folgenden Dokumenten: *Bereitstellung von virtuellen Microsoft Windows 8-Desktops mit VMware Horizon View – Anwendung von Best Practices* und *VMware Horizon View Optimization Guide for Windows 8*.

5. Installieren Sie die Drittanbietertools oder -anwendungen wie Microsoft Office, die für Ihre Umgebung relevant sind.
6. Installieren Sie den Avamar Desktop/Laptop-Client.
7. Ausführliche Informationen finden Sie im *EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View – Design- und Implementierungsleitfaden*.
8. Installieren Sie den Horizon View-Agent.

   Hinweis: Wenn Sie die View Persona Management-Funktion verwenden, installieren Sie zu diesem Zeitpunkt die Persona Management-Komponente des VMware Horizon View-Agent. Achten Sie darauf, dass die Persona Management-Option während der Installation des Horizon View-Agent ausgewählt wird.

Konfigurieren von View Persona Management-Gruppen-Policies

View Persona Management wird über Active Directory-Gruppen-Policies aktiviert, die der Organisationseinheit zugewiesen werden, die die Computerkonten für den virtuellen Desktop enthält. Die Vorlagen für die View-Gruppen-Policy befinden sich im Verzeichnis **\Program Files\VMware\VMware View\Server\extras\GroupPolicyFiles** auf dem View Connection-Server.

Konfigurieren von Gruppen-Policies für die Ordnerumleitung für EMC Avamar

Aktivieren Sie die Ordnerumleitung über die Active Directory-Gruppen-Policies, die der Organisationseinheit zugewiesen sind, die die Computerkonten für den virtuellen Desktop enthält. Die Active Directory-Ordnerumleitung wird (statt der View Persona Management-Ordnerumleitung) verwendet, damit für die Ordner die von der Avamar-Software geforderten Benennungskonsistenzen beibehalten werden. Ausführliche Informationen finden Sie im *EMC Backup und Recovery für VSPEX für Anwender-Computing für VMware Horizon View – Design- und Implementierungsleitfaden*.

Konfigurieren von View PCoIP-Gruppen-Policies

View PCoIP-Protokolleinstellungen werden über Active Directory-Gruppen-Policies gesteuert, die den Organisationseinheiten zugewiesen werden, die die View Connection-Server enthalten. **Die Vorlagen für die View-Gruppen-Policies befinden sich in der ZIP-Datei Horizon View GPO Bundle.** Verwenden Sie die Gruppen-Policy-Vorlage **pcoip.adm**, um die folgenden PCoIP-Protokolleinstellungen festzulegen:

- Maximale anfängliche Bildqualität: 70
- Maximale Bildrate: 24

Hinweis: Höhere Bildraten für die PCoIP-Sitzung und eine höhere Bildqualität können sich nachteilig auf die Serverressourcen auswirken.

Provisioning von virtuellen Desktops

Verwenden Sie View Composer in der Horizon View-Konsole, um Ihre virtuellen Desktops bereitzustellen:

1. Erstellen Sie einen automatisierten Desktop-Pool.
2. Geben Sie den bevorzugten Wert für die Option **User Assignment**: an:
   - **Dedicated**: Benutzer erhalten bei jeder Anmeldung beim Pool denselben Desktop.
   - **Floating**: Benutzer erhalten bei jeder Anmeldung zufällig aus dem Pool ausgewählte Desktops.
3. Geben Sie verknüpfte Clones von View Composer an.
4. Geben Sie einen Wert für **Pool Identification** an.
5. Konfigurieren Sie **Pool Settings** nach Bedarf.
6. Konfigurieren Sie **Provisioning Settings** nach Bedarf.
7. Akzeptieren Sie die Standardwerte für **View Composer Disks** oder bearbeiten Sie die Werte nach Bedarf.

   Wenn View Persona Management verwendet wird, wählen Sie **Do not redirect Windows profile** im Bereich Persistent Disk aus (siehe Abbildung 12).

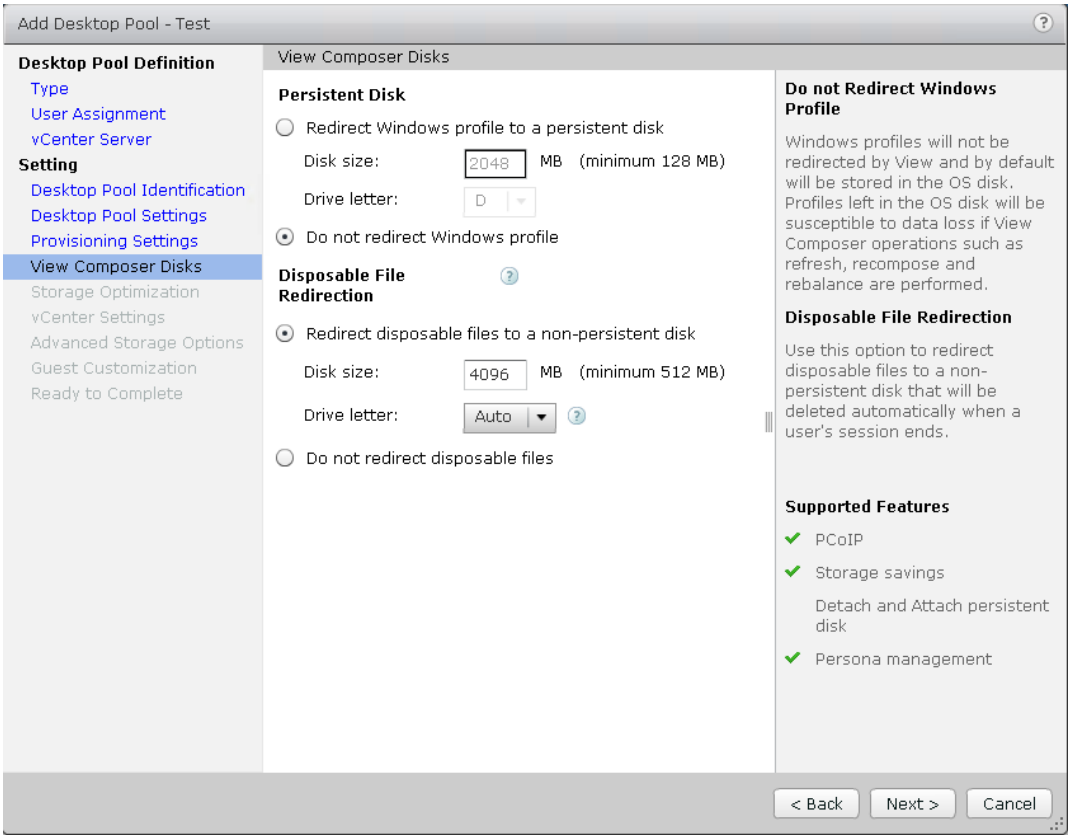

Add Desktop Pool - Test
Desktop Pool Definition
Type
User Assignment
vCenter Server
Setting
Desktop Pool Identification
Desktop Pool Settings
Provisioning Settings
View Composer Disks
Storage Optimization
vCenter Settings
Advanced Storage Options
Guest Customization
Ready to Complete
View Composer Disks
Persistent Disk
Redirect Windows profile to a persistent disk
Disk size: 2048 MB (minimum 128 MB)
Drive letter: D
Do not redirect Windows profile
Disposable File Redirection
Redirect disposable files to a non-persistent disk
Disk size: 4096 MB (minimum 512 MB)
Drive letter: Auto
Do not redirect disposable files
Do not Redirect Windows Profile
Windows profiles will not be redirected by View and by default will be stored in the OS disk. Profiles left in the OS disk will be susceptible to data loss if View Composer operations such as refresh, recompose and rebalance are performed.
Disposable File Redirection
Use this option to redirect disposable files to a non-persistent disk that will be deleted automatically when a user's session ends.
Supported Features
PCoIP
Storage savings
Detach and Attach persistent disk
Persona management
< Back
Next >
Cancel

Abbildung 12. View Composer Disks – Fenster

8. Konfigurieren Sie die Active Directory-Gruppen-Policy für View Persona Management.
9. Wählen Sie **Select separate datastores for replica and OS disk** aus.
10. Wählen Sie die entsprechende übergeordnete virtuelle Maschine, den virtuellen Maschinen-Snapshot, den Ordner, die vSphere-Hosts oder -Cluster, den vSphere-Ressourcenpool sowie die Datastores von verknüpften Clones und Laufwerkreplikaten aus.
11. Aktivieren Sie Host-Caching für den Desktop-Pool, und geben Sie Blackout-Zeiten für die Cacheregeneration an.
12. Geben Sie Image-Anpassungsoptionen nach Bedarf an.
13. Schließen Sie den Poolerstellungsprozess ab, um die Erstellung des virtuellen Desktop-Pools zu initiieren.

Einrichten von EMC Avamar

Wenn Ihre Lösung Avamar Datensicherheit enthält, finden Sie ausführliche Informationen zur Implementierung Ihrer VSPEX-Lösung im *EMC Backup und Recovery für VSPEX für Anwender-Computing für VMware Horizon View – Design- und Implementierungsleitfaden*.

Einrichten von VMware vShield Endpoint

In diesem Abschnitt werden Informationen zum Einrichten und Konfigurieren der Komponenten von vShield Endpoint bereitgestellt. In Tabella 13 beschreibt die Aufgaben, die abgeschlossen werden müssen.

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für VMware vShield Endpoint in den Pool der EMC VSPEX Private Cloud zu integrieren. Die empfohlene CPU- und Arbeitsspeicherkonfiguration finden Sie in der *vShield-Kurzanleitung*.

Tabella 13. Für die Installation und Konfiguration von vShield Endpoint erforderliche Aufgaben

Aufgabe	Beschreibung	Referenz	
Überprüfen der Desktoptreiberinstallation für vShield Endpoint	Überprüfen Sie, ob die vShield Endpoint-Treiberkomponente von VMware Tools auf dem virtuellen Desktop Master Image installiert wurde.	Überprüfen der Desktop-Treiberinstallation für vShield Endpoint auf Seite 48	*vShield-Kurzanleitung*
Bereitstellen der vShield Manager-Appliance	Führen Sie die Bereitstellung und Konfiguration der vShield Manager-Appliance durch und registrieren Sie sie beim vSphere-Client.	Bereitstellen der vShield Manager-Appliance auf Seite 48	
Anwenden von vShield Endpoint-Lizenzen	Wenden Sie die vShield Endpoint-Lizenzschlüssel über das vCenter-Lizenzdienstprogramm an.	Anwenden von vShield Endpoint-Lizenzen auf Seite 48	
Installieren des vSphere vShield Endpoint-Services	Installieren Sie den vShield Endpoint-Service auf den vSphere-Desktop-Hosts.	Installieren des vShield Endpoint-Services auf Seite 48	
Bereitstellen eines Management-servers für die Virenschutzlösung	Führen Sie die Bereitstellung und Konfiguration eines Managementservers für die Virenschutzlösung durch.	Bereitstellen eines Management-servers für die Virenschutzlösung auf Seite 48	*vShield-Kurzanleitung* **Hinweis**: Die Management-Serversoftware für die Virenschutzlösung und virtuellen Sicherheitsmaschinen werden von vShield Endpoint-Partnern bereitgestellt. Genaue Details zur Installation und Konfiguration finden Sie in der Dokumentation des Anbieters.
Bereitstellen der virtuellen vSphere-Sicherheitsmas-chinen	Führen Sie die Bereitstellung und Konfiguration der virtuellen Sicherheitsmaschinen auf jedem vSphere-Desktop-Host durch.	Bereitstellen der virtuellen vSphere-Sicherheits-maschinen auf Seite 48	
Überprüfen der vShield Endpoint-Funktion	Überprüfen Sie die Funktion der vShield Endpoint-Komponenten mithilfe des virtuellen Desktop-Master-Image.	Überprüfen der vShield Endpoint-Funktion auf Seite 49	**Hinweis**: Details zur Überprüfung der vShield Endpoint-Integration und -Funktion finden Sie in der Dokumentation des Anbieters.

Überprüfen der Desktop-Treiberinstallation für vShield Endpoint

Der vShield Endpoint-Treiber ist eine Subkomponente des VMware Tools-Softwarepakets, das auf dem virtuellen Desktop Master Image installiert ist. Installieren Sie den Treiber mithilfe einer der folgenden Methoden:

- Wählen Sie während der VMware Tools-Installation die Option **Complete** aus.
- Wählen Sie während der VMware Tools-Installation die Option **Custom** aus. Wählen Sie aus dem Listenfeld **VMware Device Drivers** die Option **VMCI Driver** und dann **vShield Driver** aus.

Zum Installieren des vShield Endpoint-Treibers auf einer virtuellen Maschine, auf der VMware Tools bereits installiert ist, initiieren Sie die VMware Tools-Installation und wählen Sie die entsprechende Option aus.

Bereitstellen der vShield Manager-Appliance

Die vShield Manager-Appliance wird von VMware als OVA-Datei bereitgestellt, die über den vShield-Client mithilfe von **File – Deploy OVF template** importiert wird. Die vShield Manager-Appliance ist mit allen erforderlichen Komponenten vorkonfiguriert.

Anwenden von vShield Endpoint-Lizenzen

Das vCenter-Lizenzdienstprogramm wird verwendet, um die vShield Endpoint-Lizenzschlüssel anzuwenden.

Installieren des vShield Endpoint-Services

Der vShield Endpoint-Service muss auf allen virtuellen vSphere-Desktophosts installiert sein. Der Service wird auf den vSphere-Hosts von der vShield Manager-Appliance installiert. Die vShield Manager-Webkonsole wird für die Initiierung der vShield Endpoint-Serviceinstallation und zur Überprüfung der erfolgreichen Installation verwendet.

Bereitstellen eines Management-servers für die Virenschutzlösung

Der Managementserver für die Virenschutzlösung wird für das Management der Virenschutzlösung verwendet und von vShield Endpoint-Partnern bereitgestellt. Der Managementserver und damit verbundene Komponenten sind eine erforderliche Komponente der vShield Endpoint-Plattform.

Bereitstellen der virtuellen vSphere-Sicherheits-maschinen

Die virtuellen vSphere-Sicherheitsmaschinen (SVMs) werden von den vShield Endpoint-Partnern bereitgestellt und auf jedem virtuellen vSphere-Desktophost installiert. Die virtuellen Sicherheitsmaschinen führen sicherheitsrelevante Vorgänge für alle virtuellen Desktops aus, die sich auf ihrem vSphere-Host befinden. Die virtuellen Sicherheitsmaschinen und damit verbundene Komponenten sind erforderliche Komponenten der vShield Endpoint-Plattform.

Überprüfen der vShield Endpoint-Funktion

Nachdem alle erforderlichen Komponenten der vShield Endpoint-Plattform installiert und konfiguriert wurden, überprüfen Sie die Funktion der Plattform, bevor Sie die virtuellen Desktops bereitstellen.

Überprüfen Sie mithilfe der vom vShield Endpoint-Partner bereitgestellten Dokumentation die Funktion der vShield Endpoint-Plattform mit dem Master Image des virtuellen Desktop.

Einrichten von VMware Horizon Workspace

In diesem Abschnitt finden Sie Informationen zur Einrichtung und Konfiguration von VMware Horizon Workspace für die Lösung. Für eine Neuinstallation von Horizon Workspace empfiehlt VMware, dass Sie die Aufgaben in der in Tabella 12 angegebenen Reihenfolge durchführen.

Zusätzlich zu den Referenzen, die in diesem Abschnitt enthalten sind, bietet die VMware Horizon Workspace-Dokumentation die zusätzlichen Informationen, die erforderlich sind, um die Installation und Konfiguration der VMware Horizon Workspace abzuschließen.

Hinweis: EMC empfiehlt, die Horizon Workspace vApp in den Pool der VSPEX Private Cloud zu integrieren.

Tabella 14. Aufgaben für die Einrichtung von VMware Horizon Workspace

Aufgabe	Beschreibung	Referenz
Zuweisen von IP-Adressen und Erstellen von DNS-Datensätzen	Für jede virtuelle Appliance von Horizon Workspace ist eine IP-Adresse erforderlich.	Zuweisen von IP-Adressen und Erstellen von DNS-Datensätzen auf Seite 52
Gewähren der SMTP-Relayberechtigungen für Workspace-Appliances	Horizon Workspace muss SMTP-Nachrichten bezüglich Benutzerkontoinformationen und Warnmeldungen senden können.	• Gewähren der SMTP-Relayberechti-gungen für Workspace auf Seite 52 • E-Mail-Serverdokumentation
Konfigurieren einer PostgreSQL- oder Oracle-Datenbank für Workspace	Horizon Workspace speichert kritische Konfigurationsinformationen in einer Datenbank. Eine externe Datenbank wird aus Performance- und Skalierungsgründen empfohlen.	Konfigurieren einer PostgreSQL- oder Oracle-Datenbank für Workspace auf Seite 52
Konfigurieren einer CIFS-Freigabe zur Verwendung als ThinApp-Repository (optional)	Um die Verteilung der Anwendungen, die in VMware ThinApp enthalten sind, zu aktivieren, ist die Dateifreigabe mit Leseberechtigung für Horizon-Benutzer erforderlich.	• Konfigurieren einer CIFS-Freigabe zur Verwendung als ThinApp-Repository (optional) auf Seite 52 • *EMC VNXe3200 – Installationshandbuch* • *Leitfaden für die ersten Schritte mit dem Unisphere-System*

Aufgabe	Beschreibung	Referenz
Verifizieren der angegebenen E-Mail-Adressen aller Workspace-Benutzer	Horizon Workspace erfordert, dass Benutzer E-Mail-Adressen angeben.	Verifizieren der angegebenen E-Mail-Adressen aller Workspace-Benutzer auf Seite 53
Bereitstellen der Workspace-Portal-Appliance für vCenter	Horizon Workspace vApp wird als OVA-Datei bereitgestellt, die die Dateien enthält, die erforderlich sind, um die Horizon Workspace-Appliance bereitzustellen.	Bereitstellen der Workspace-Appliance für vCenter auf Seite 53
Optional; Bereitstellen einer zweiten Workspace-Portal-Appliance für vCenter	In Kombination mit einer Lastenausgleichslösung kann eine zweite Workspace-Portal-Appliance zur Aktivierung von Lastenausgleich und zur hohen Verfügbarkeit für Horizon Workspace eingesetzt werden.	*Erweiterte Konfiguration für VMware Workspace Portal Appliance*
Erstellen eines Active Directory-Kontos, das für die Workspace Active Directory-Integration verwendet wird	Dieses Konto wird von Horizon dafür verwendet, Active Directory-Kontodaten zu synchronisieren, und muss sich innerhalb der Organisationseinheit befinden, die die Horizon-Zielbenutzer enthält.	Windows-Dokumentation auf Microsoft TechNet-Website
Erlangen der Informationen, die erforderlich sind, um die Workspace-Integration mit Active Directory zu aktivieren	Horizon Workspace muss auf Active Directory zugreifen können, sodass es Benutzerkonten und Active Directory-Gruppen auflösen kann.	Erlangen der Informationen, die erforderlich sind, um die Workspace-Integration mit Active Directory zu aktivieren auf Seite 53
Erstellen eines Active Directory-Kontos, das für die Workspace vCenter-Integration verwendet wird	Dieses Konto wird von Horizon verwendet, um die VMware vCenter-Server-Integration durchzuführen.	Anbieterdokumentation
Erlangen der Informationen, die erforderlich sind, um die Workspace-Integration mit VMware vCenter zu aktivieren	Es werden u. a. folgende Informationen benötigt: • vCenter-Hostname-FQDN • vCenter-Port-Nummer • Benutzername für das zuvor erstellte Horizon Workspace vCenter-Integrationskonto • Passwort für das zuvor erstellte Horizon Workspace vCenter-Integrationskonto	
Erlangen des Workspace-Lizenzschlüssels	Der Lizenzschlüssel wird von VMware zur Verfügung gestellt und aktiviert die Horizon Workspace-Plattform.	

Aufgabe	Beschreibung	Referenz
Verwenden des Workspace-Administrations-Webportals zum Abschließen der webbasierten UI-Installation.	Das Workspace-Administrations-Webportal finden Sie unter https://*workspace-va-FQDN:8443.*	
Verwenden eines vertrauenswürdigen SSL-Zertifikats und eines privaten Schlüssels für die virtuellen Workspace-Maschinen (optional)	Standardmäßig installiert Workspace ein selbst signiertes SSL-Zertifikat, dem weder Webclients noch Computer mit der Workspace-Software vertrauen. Das Zertifikat muss ersetzt werden, um diese Fehler zu vermeiden.	Verwenden eines vertrauenswürdigen SSL-Zertifikats und eines privaten Schlüssels für die Workspace-Appliance (optional) auf Seite 53
Aktivieren von RSA SecurID-basierter Authentifizierung (optional)	Workspace unterstützt RSA SecurID als Authentifizierungsmechanismus. Um diese Option zu aktivieren, greifen Sie auf das Workspace-Administrations-Webportal unter https://*workspace-va-FQDN* zu.	RSA-Dokumentation
Konfigurieren des externen Zugriffs auf die Workspace-Appliance (optional)	Um den externen Zugriff für andere Horizon Workspace-Komponenten zu aktivieren, benötigen Sie Zugriff auf die Horizon Workspace-Appliance.	• Konfigurieren des externen Zugriffs auf die Workspace-Appliance (optional) auf Seite 54 • Firewall-Herstellerdokumentation
Aktivieren der Horizon View-Integration (optional)	Bei Integration in Horizon View können Horizon Workspace-Benutzer auf ihre View-Desktops direkt vom Horizon Workspace-Portal aus zugreifen.	Aktivieren der Horizon View-Integration (optional) auf Seite 54
Aktivieren von ThinApp-Paketen (optional)	Workspace bietet Ihnen die Möglichkeit, Anwendungen automatisch mithilfe von ThinApp als Pakete für Clients zu verteilen, die den Horizon-Agent ausführen, oder diese Anwendungen auf Anfrage an Webclients zu streamen.	• *VMware Workspace Portal – Administratorhandbuch* • *Einrichten von Ressourcen in VMware Workspace Portal* • *VMware Workspace Portal – Anwenderhandbuch*
Aktivieren von Webanwendungen (optional)	Arbeitsumgebung umfasst einen Katalog mit Webanwendungen, die mit dem Workspace-Portal eingesetzt werden können.	
Aktivieren von Citrix-veröffentlichten Anwendungen (optional)	Workspace kann in Citrix XenApp integriert werden, um Zugriff auf Anwendungen, die durch diese Plattform gehostet werden, zu ermöglichen.	

Aufgabe	Beschreibung	Referenz
Benutzern erlauben, Horizon Workspace-Funktionen zu verwenden	Workspace-Benutzer verfügen standardmäßig nicht über die Berechtigung, die Funktionen von Horizon Workspace zu verwenden. Verwenden Sie das Workspace-Dashboard, um Richtlinien zu erstellen und Active Directory-Benutzern und -Gruppen Zugriff auf Workspace-Funktionen zu gewähren.	
Erfassen von Anwendungen mithilfe von VMware ThinApp (optional)	Mithilfe von VMware ThinApp erfasste Anwendungen können in das Workspace ThinApp-Repository hochgeladen und Clients zur Verfügung gestellt werden, die Workspace-Policies verwenden.	• *ThinApp – Benutzerhandbuch* • *ThinApp Package.ini-Parameter – Referenzleitfaden*

Zuweisen von IP-Adressen und Erstellen von DNS-Datensätzen

Die DNS-Datensätze zu den Horizon Workspace-Anwendungen müssen vor der Bereitstellung mithilfe der gewünschten IP-Adressen für jede Anwendung erstellt werden. Sowohl Forward (A)- als auch Reverse (PTR)-Datensätze sollten erstellt werden.

Gewähren der SMTP-Relayberechtigungen für Workspace

Die Horizon Workspace-Appliance muss dazu in der Lage sein, Nachrichten mit einem SMTP-Server zu übermitteln. Konfigurieren Sie zu diesem Zweck eine vorhandene E-Mail-Adresse und vergewissern Sie sich, dass die Appliance die erforderlichen Berechtigungen hat.

Konfigurieren einer PostgreSQL- oder Oracle-Datenbank für Workspace

Während der Erstkonfiguration von Horizon Workspace werden Sie dazu aufgefordert, die standardmäßige eingebettete PostgreSQL-Datenbank oder eine Datenbank zu verwenden, die auf einem dedizierten Server gehostet wird, auf dem entweder eine unterstützte Version von Oracle oder PostgreSQL ausgeführt wird. Wir empfehlen, dass Sie einen dedizierten Server verwenden, um die Workspace-Datenbank für Performance- und Managementzwecke zu hosten.

Sie müssen die Datenbank vor der Konfiguration der Horizon Workspace erstellen, indem Sie die folgenden Anweisungen befolgen, die Sie im Dokument *Installieren und Konfigurieren von VMware Workspace Portal* finden. Die Datenbank benötigt 64 GB Speicherplatz und kann Horizon Workspace-Umgebungen mit bis zu 100.000 Benutzern umfassen.

Konfigurieren einer CIFS-Freigabe zur Verwendung als ThinApp-Repository (optional)

Wenn Sie Horizon Workspace dafür verwenden, Anwendungen bereitzustellen, die mit VMware ThinApp zusammengestellt wurden, erstellen Sie eine CIFS- oder Windows-Freigabe für die Speicherung von Anwendungen. Der Platzbedarf hängt von der Anzahl der Pakete ab, die von der Freigabe gehostet werden.

Wenn Sie VNXe dafür verwenden, die ThinApp-Freigabe zu hosten, erstellen Sie das erforderliche Dateisystem innerhalb des Infrastrukturserver-Speicherpools und anschließend eine CIFS-Freigabe. Horizon Workspace-Benutzer benötigen schreibgeschützten Zugriff auf diese Freigabe, während ThinApp-Administratoren Lese-/Schreibzugriff benötigen, um ThinApp-Pakete zu verwalten.

Verifizieren der angegebenen E-Mail-Adressen aller Workspace-Benutzer

Horizon Workspace erfordert, dass alle Benutzer eine E-Mail-Adresse in ihrem Active Directory-Konto angeben. Wenn das Active Directory-E-Mail-Adressfeld leer ist, werden Benutzer nicht für Horizon Workspace aktiviert.

Das Active Directory-Konto muss nicht E-Mail-fähig sein. Das ist ein Begriff, der für Unternehmen verwendet wird, die Microsoft Exchange verwenden. Nur Horizon Workspace erfordert, dass das Active Directory-E-Mail-Adressfeld des Benutzers eine gültige E-Mail-Adresse enthält.

Bereitstellen der Workspace-Appliance für vCenter

Wenn Sie die Deploy OVF Template-Funktion in der vCenter-Konsole verwenden, stellen Sie die Horizon Workspace-Portal-Appliance bereit. Legen Sie dazu folgende Feldwerte fest:

- **Hostname (FQDN)** – Der FQDN für die Horizon Gateway-Appliance.
- **Standardgateway**
- **DNS** – Active Directory-Domain-DNS-Server; wenn IP-Adressen von mehreren Servern vorhanden sind, trennen Sie sie durch ein Komma.
- **IP-Adresse** – IP-Adresse für die Workspace-Appliance.
- **Netzmaske**
- **Diskformat** – Thin Provisioning
- **Netzwerkzuordnung** – Zielnetzwerk für die virtuelle Workspace-Appliance

Erlangen der Informationen, die erforderlich sind, um die Workspace-Integration mit Active Directory zu aktivieren

Horizon Workspace erfordert, dass sich die Acitve Directory-Benutzerkonten in einer Organisationseinheit befinden, die sich von der standardmäßigen Anwenderorganisationseinheit unterscheidet, und zwar wie folgt:

- Name des Active Directory-Domain Controllers und FQDN
- Active Directory-Kontext für die Anbindung; das Stammverzeichnis der Active Directory-Organisationseinheit, die Horizon-Benutzer und -Gruppen enthält, z. B.:

  OU=HorizonWorkspace,DC=rtp,DC=lab,DC=emc,DC=com
- Active Directory-Basis-DN des zuvor erstellten Horizon Workspace Active Directory-Integrationskontos, z. B.:

  CN=svc-horizon,OU=HorizonWorkspace,DC=rtp,DC=lab,DC=emc,DC=com
- Passwort für das zuvor erstellte Horizon Workspace Active Directory-Integrationskonto
- Active Directory-Benutzername und -Passwort eines Kontos mit Rechten, Computer mit der Domain zu verknüpfen

Verwenden eines vertrauenswürdigen SSL-Zertifikats und eines privaten Schlüssels für die Workspace-Appliance (optional)

Sie können ein vertrauenswürdiges SSL-Zertifikat und einen dazugehörigen privaten Schlüssel verwenden, um das Horizon Workspace-Appliance-Standard-SSL-Zertifikat zu ersetzen. Wenn das Zertifikat nicht ersetzt wird, können Clients auf SSL-Validierungsfehler stoßen, wenn sie auf die Horizon Workspace-Umgebung zugreifen. Die Root- und Zwischenzertifikate sind ebenfalls erforderlich, um den Zertifikataustauschprozess abzuschließen.

Sie können ein einzelnes Platzhalterzertifikat verwenden oder individuelle Personenzertifikate auf jeder virtuellen Workspace-Maschine ersetzen. Die Zertifikate sollten das PEM-Format (Privat Enhanced Mail) aufweisen.

Konfigurieren des externen Zugriffs auf die Workspace-Appliance (optional)

Horizon Workspace muss über das Internet erreichbar sein, um Funktionen wie die Nutzung von Horizon Workspace als Gateway für den externen Zugriff auf VMware Horizon View zu ermöglichen.

Wenn diese Funktionen erforderlich sind, konfigurieren Sie den externen Zugriff, wie in *Installieren und Konfigurieren von Horizon Workspace* beschrieben.

Aktivieren der Horizon View-Integration (optional)

Wenn Horizon Workspace als Gateway für den Zugriff auf VMware Horizon View verwendet wird, müssen Sie die View-Integration in der Horizon Workspace-Konsole sowie die SAML-Authentifikation in VMware Horizon View aktivieren.

Einrichten von VMware vCenter Operations Manager for Horizon View

In diesem Kapitel erhalten Sie Informationen zum Einrichten und Konfigurieren von VMware vCenter Operations Manager for Horizon View. In Tabella 15 beschreibt die Aufgaben, die abgeschlossen werden müssen.

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für den VMware vCenter Operations Manager for Horizon View-Server in den Pool der VSPEX Private Cloud zu integrieren. Im *VMware vCenter Operations Manager für Horizon View – Installations- und Konfigurationsleitfaden* finden Sie die empfohlene CPU- und Speicherkonfiguration.

Tabella 15. Für die Installation und Konfiguration von vCenter Operations Manager erforderliche Aufgaben

Aufgabe	Beschreibung	Referenz
Erstellen eines vSphere-IP-Pools für vCenter Operations Manager	Erstellen Sie einen IP-Pool mit 2 verfügbaren IPs zur Verwendung für die vCenter Operations Manager-Analyse und die Benutzeroberfläche der virtuellen Maschinen.	• *VMware vCenter Operations Manager für Horizon View – Installations- und Konfiguration-shandbuch* • *VMware vCenter Operations Manager für Horizon View – Administratorhand-buch* • *VMware vCenter Operations Manager für Horizon View – Sicherheitshand-buch*
Bereitstellen von vCenter Operations Manager vSphere Application Services (vApp)	Führen Sie die Bereitstellung und Konfiguration der vCenter Operations Manager vApp durch. Passen Sie die Spezifikationen der zwei virtuellen Server, die vCenter Operations Manager vApp umfassen, abhängig von der Anzahl der überwachten virtuellen Maschinen an.	
Angeben des zu überwachenden vCenter-Servers	Geben Sie auf der Hauptweboberfläche von vCenter Operations Manager den Namen des vCenter-Servers an, der die virtuellen Desktops managt.	

Aufgabe	Beschreibung	Referenz
Zuweisen der vCenter Operations Manager-Lizenz	Wenden Sie die vCenter Operations Manager for Horizon View-Lizenzschlüssel über das vCenter-Lizenzdienstprogramm an.	
Konfigurieren der SNMP- und SMTP-Einstellungen	Konfigurieren Sie über die Hauptweboberfläche von vCenter Operations Manager alle für Überwachungszwecke erforderlichen SNMP- oder SMTP-Einstellungen. **Hinweis**: Diese Einstellung ist optional.	
Aktualisieren der Einstellungen für den virtuellen Desktop	Aktualisieren Sie Firewall-Policies und -services für den virtuellen Desktop, um das Erfassen von für vCenter Operations Manager for Horizon View-Desktops spezifischen Kennzahlen zu unterstützen.	
Erstellen der virtuellen Maschine für den vCenter Operations Manager für Horizon View-Adapterserver	Erstellen Sie eine virtuelle Maschine im vSphere-Client, die als vCenter Operations Manager for Horizon View Adapter-Server verwendet wird.	
Installieren des Gastbetriebssystems für den vCenter Operations Manager für Horizon View-Adapterserver	Installieren Sie Windows-Server 2012 R2 als Gastbetriebssystem für den vCenter Operations Manager für Horizon View-Adapterserver.	
Installieren der VMware vCenter Operations Manager für Horizon View Adapter-Software	Führen Sie die Bereitstellung und Konfiguration der vCenter Operations Manager for Horizon View Adapter-Software durch.	
Importieren der vCenter Operations Manager für Horizon View-PAK-Datei	Importieren Sie die vCenter Operations Manager for Horizon View Adapter-PAK-Datei über die Hauptweboberfläche von vCenter Operations Manager.	
Überprüfen der VMware vCenter Operations Manager für Horizon View-Funktionalität	Überprüfen Sie die Funktion von vCenter Operations Manager for Horizon View über das Master-Image des virtuellen Desktops.	

Kapitel 5 Lösungsverifizierung

In diesem Kapitel werden folgende Themen behandelt:

Überblick **58**

Checkliste nach der Installation **59**

Bereitstellen und Testen eines einzigen virtuellen Desktops **59**

Überprüfen der Redundanz der Lösungskomponenten **59**

Überblick

Nachdem Sie die Lösung konfiguriert haben, führen Sie die Aufgaben in Tabella 16 durch, um die Konfiguration und Funktionen spezifischer Aspekte der Lösung zu überprüfen und sicherzustellen, dass die Konfiguration die zentralen Verfügbarkeitsanforderungen erfüllt.

Tabella 16. Aufgaben für das Testen der Installation

Aufgabe	Beschreibung	Referenz
Überprüfen der Installation mit der Checkliste nach der Installation	Überprüfen Sie, ob geeignete virtuelle Ports auf jedem virtuellen vSphere-Host-Switch vorhanden sind.	• Checkliste nach der Installation auf Seite 59 • *Handbuch für vSphere-Netzwerk* • *vSphere-Speicher*
	Überprüfen Sie, ob jeder vSphere-Host auf die erforderlichen Datastores und VLANs zugreifen kann.	
	Überprüfen Sie, ob die vMotion-Schnittstellen auf allen vSphere-Hosts korrekt installiert sind.	
Bereitstellen und Testen eines einzigen virtuellen Desktops	Stellen Sie eine einzige virtuelle Maschine über die vSphere-Oberfläche bereit und verwenden Sie dabei die Anpassungsspezifikation.	• Bereitstellen und Testen eines einzigen virtuellen Desktops auf Seite 59 • *Handbuch für vCenter Server- und Hostverwaltung* • *vSphere-Handbuch für die Verwaltung virtueller Maschinen*
Überprüfen der Redundanz der Lösungskomponenten	Starten Sie jeden SP nacheinander neu und achten Sie darauf, dass die Verbindung mit den VMware-Datastores aufrechterhalten wird.	• Überprüfen der Redundanz der Lösungskomponenten auf Seite 59 • Dokumentation des Anbieters • *Handbuch für vCenter Server- und Hostverwaltung*
	Deaktivieren Sie nacheinander jeden der redundanten Switches, und überprüfen Sie, ob die Verbindung von vSphere-Host, virtueller Maschine und Speicher-Array intakt bleibt.	
	Aktivieren Sie auf einem vSphere-Host, der mindestens eine virtuelle Maschine enthält, den Wartungsmodus, und überprüfen Sie, ob die virtuelle Maschine erfolgreich zu einem alternativen Host migrieren kann.	
Provisioning der verbleibenden virtuellen Desktops	Stellen Sie Desktops über die verknüpften View Composer-Clones bereit.	• *Verwaltung von VMware Horizon View*

Checkliste nach der Installation

Die folgenden Konfigurationselemente sind wichtig für die Funktion der Lösung und sollten vor der Bereitstellung in die Produktion überprüft werden. Überprüfen Sie Folgendes auf jedem vSphere-Server, der als Teil dieser Lösung verwendet wird:

- Die vSwitche, die die Client-VLANs hosten, sind mit ausreichend Ports konfiguriert, um die maximale Anzahl an virtuellen Maschinen zu beherbergen, die ein Host hosten kann.
- Alle erforderlichen virtuellen Maschinenportgruppen sind konfiguriert, und jeder Server kann auf die erforderlichen VMware-Datastores zugreifen.
- Für vMotion ist eine ordnungsgemäß konfigurierte Schnittstelle vorhanden. Ausführliche Informationen finden Sie in *vSphere-Netzwerk*.

Weitere Informationen finden Sie in der Liste von Dokumenten in Kapitel 6, Referenzdokumentation, auf Seite 61 .

Bereitstellen und Testen eines einzigen virtuellen Desktops

Stellen Sie eine einzige virtuelle Maschine bereit, um den Betrieb der Lösung zu überprüfen. Überprüfen Sie, ob die virtuelle Maschine der entsprechenden Domain zugeordnet ist, Zugriff auf die erwarteten Netzwerke hat und es möglich ist, sich bei ihr anzumelden.

Überprüfen der Redundanz der Lösungskomponenten

Testen Sie bestimmte Szenarien, die für die Wartung oder Hardwareausfälle relevant sind, wie folgt, um zu überprüfen, ob die verschiedenen Komponenten der Lösung die Verfügbarkeitsanforderungen erfüllen.

1. Starten Sie jeden VNXe-SP nacheinander neu und überprüfen Sie, ob die Verbindung zu den VMware-Datastores während des Vorgangs aufrechterhalten wird. Führen Sie die folgenden Schritte aus:
   a. Melden Sie sich mit Administrator-Anmeldedaten bei SP A an.
   b. Starten Sie SP A über den Befehl `svc_shutdown -r` neu.
   c. Überprüfen Sie während des Neustartzyklus die Präsenz von Datastores auf ESXi-Hosts.
   d. Wenn der Zyklus abgeschlossen ist, melden Sie sich bei SP B an und starten Sie ihn über den Befehl `svc_shutdown -r` neu.
2. Aktivieren Sie auf einem vSphere-Host, der mindestens eine virtuelle Maschine enthält, den Wartungsmodus, und überprüfen Sie, ob die virtuelle Maschine zu einem alternativen Host migriert werden kann.

Kapitel 6 Referenzdokumentation

In diesem Kapitel werden folgende Themen behandelt:

EMC Dokumentation **62**

Andere Dokumentation **62**

EMC Dokumentation

Die folgenden Dokumente auf der EMC Online Support-Website bieten weitere und relevante Informationen. Der Zugriff auf diese Dokumente hängt von Ihren Anmeldedaten ab. Falls Sie auf ein Dokument nicht zugreifen können, wenden Sie sich an Ihren EMC Vertriebsmitarbeiter:

- *EMC VNXe3200–Installationshandbuch*
- *EMC VSI für VMware vSphere Web Client – Produktleitfaden*
- *Konfigurationsarbeitsblatt für die VNXe-Serie*
- *Bereitstellung von virtuellen Microsoft Windows 8-Desktops – Leitfaden zur Anwendung von Best Practices*
- *Installations- und Administrationshandbuch für PowerPath/VE für VMware vSphere*

Andere Dokumentation

Die folgenden Dokumente auf der VMware-Website bieten weitere und relevante Informationen:

- *Bereitstellungs- und Konfigurationsleitfaden für vCenter Operations Manager 5.8*
- *VMware vSphere – Installations- und Einrichtungshandbuch*
- *VMware vSphere-Netzwerk*
- *Handbuch zur VMware vSphere-Ressourcenverwaltung*
- *VMware vSphere-Speicher – Handbuch*
- *vSphere-Administratorhandbuch für virtuelle Maschinen*
- *VMware vSphere-Handbuch für die Verwaltung virtueller Maschinen*
- *Handbuch für VMware vCenter Server- und Hostverwaltung*
- *Installieren und Verwalten von VMware vSphere Update Manager*
- *Vorbereiten der Update Manager-Datenbank*
- *Vorbereiten der vCenter Server-Datenbanken*
- *Management von Arbeitsspeicherressourcen in VMware vSphere 5.0*
- *View – Erste Schritte*
- *View – Planung der Technologie*
- *View – Installation*
- *Szenarien für die Einrichtung von SSL-Zertifikaten für View*
- *Einrichten von Desktop- und Anwendungspools in View*
- *Verwalten der View-Cloud-Pod-Architektur*
- *View – Migration von Benutzerprofilen*
- *View Security*
- *View – Migration von Benutzerprofilen*

- *VMware Horizon View 6.0 – Versionshinweise*
- *VMware Horizon View Optimization Guide for Windows 7 and Windows 8*
- *Installieren und Konfigurieren von VMware Workspace Portal*
- *Migration von VMware Workspace Portal*
- *VMware Workspace Portal – Administratorhandbuch*
- *Einrichten von Ressourcen in VMware Workspace Portal*
- *VMware Workspace Portal – Anwenderhandbuch*
- *Administratorhandbuch für VMware vCenter Operations Manager*
- *VMware vCenter Operations Manager for View Installation Guide*
- *Installationshandbuch für VMware vCenter Operations Manager*
- *Bereitstellungs- und Konfigurationsleitfaden für vCenter Operations Manager*
- *VMware vShield – Administratorhandbuch*
- *VMware vShield – Kurzanleitung*

Anhang A Konfigurationsarbeitsblatt

In diesem Anhang wird das folgende Thema behandelt:

Arbeitsblatt für die Kundenkonfiguration 66

Arbeitsblatt für die Kundenkonfiguration

Bevor Sie die Lösung konfigurieren, müssen Sie einige kundenspezifische Konfigurationsinformationen wie IP-Adressen, Hostnamen und so weiter erfassen. Sie können Tabella 17 bis Tabella 22 in diesem Anhang als Arbeitsblatt verwenden, um die Informationen aufzuzeichnen. Sie können das Arbeitsblatt auch ausdrucken und dem Kunden als zukünftige Referenz überlassen.

Im Anhang zu diesem Dokument finden Sie eine eigenständige Kopie des Arbeitsblatts im Microsoft Office Word-Format. So zeigen Sie das Arbeitsblatt an und drucken es aus:

1. Öffnen Sie in Adobe Reader den Bereich **Attachments** wie folgt:
   - Wählen Sie **View** › **Show/Hide** › **Navigation Panes** › **Attachments** aus.

     oder
   - Klicken Sie auf das Symbol **„Attachments“**, wie in Abbildung 13 dargestellt.

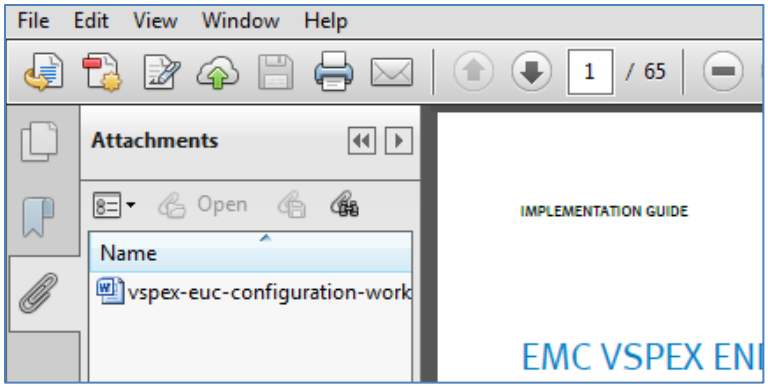


Abbildung 13. Öffnen von Anhängen in einer PDF-Datei

2. Doppelklicken Sie unter **Attachments** auf die angehängte Datei, um das Arbeitsblatt zu öffnen und auszudrucken.

Um die Kundeninformationen zu bestätigen, überprüfen Sie das *Konfigurationsarbeitsblatt für die VNXe-Serie*.

Tabella 17. Allgemeine Serverinformationen

Servername	Zweck	Primäre IP-Adresse
	Domain Controller	
	Primäres DNS	
	Sekundäres DNS	
	DHCP	
	NTP	
	SMTP	
	SNMP	
	VMware vCenter-Konsole	
	VMware Horizon View Connection Server	
	VMware Horizon Workspace-Appliance(s)	

Servername	Zweck	Primäre IP-Adresse
	Microsoft SQL Server	
	VMware vShield Manager	
	Managementserver für die Virenschutzlösung	

Tabella 18. vSphere-Serverinformationen

Servername	Zweck	Primäre IP-Adresse	Private Netzadresse (Speicher)	VMkernel-IP-Adresse	vMotion-IP-Adresse
	vSphere-Host 1				
	vSphere Host 2				
	...				

Tabella 19. Array-Informationen

Feld	Wert
Arrayname	
Administratorkonto	
Management-IP-Adresse	
Name des Speicherpools	
Name des Datastore	
IP-Adresse des NFS-Servers	

Tabella 20. Informationen zur Netzwerkinfrastruktur

Vorname	Zweck	IP-Adresse	Subnetzmaske	Standard-Gateway
	Ethernet Switch 1			
	Ethernet Switch 2			
	...			

Tabella 21. VLAN-Informationen

Vorname	Zweck des Netzwerks	VLAN ID	Zugelassene Subnetze
	Clientzugriffsnetzwerk		
	Speichernetzwerk		
	Managementnetzwerk		

Tabella 22. Servicekonten

aufrufen	Zweck	Passwort (optional, angemessen gesichert)
	Windows Server-Administrator	
Root	vSphere-Root	
Root	Array Root	
	Array-Administrator	
	VMware vCenter-Administrator	
	VMware Horizon View-Administrator	
	VMware Horizon Workspace – Gebundenes Konto	
Admin	VMware Horizon Workspace-Appliance-Admin-Konto	
Root	VMware Horizon Workspace-Appliance-Root-Konto	
Sshuser	VMware Horizon Workspace-Appliance-sshuser-Konto	
	SQL Server-Administrator	
	VMware vCenter Operations Manager-Administrator	
	VMware vShield Manager-Administrator	